8 Authentication Trends

of The Online Payments Industry in 2018 and Beyond

GPayments

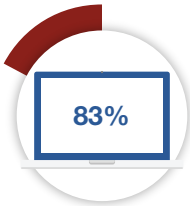
authentication, security and payment solutions

CONTENTS

BACKGROUND

The boom in the internet and mobile economy means that online identity authentication has steadily grown into one of the biggest challenges business owners, payment providers, card issuers and, most importantly, customers must deal with on an almost daily basis. The risk of getting it wrong is nowhere greater than within the scope of online payments.

Own Smartphone



Own Laptop

Digital Commerce

91% of consumers own a smartphone and 83% own a laptop. With 90% of activities relating to digital commerce, most of the time spent on these devices is for buying goods and services online[1].

As a result, online retail sales are expected to grow to $2.489 trillion by the end of 2018, up 13.29% (or almost $300 billion) from 2017's $2.197 trillion[2].

At the same time, eCommerce fraud attacks rose 30% during 2017[3], with public estimates putting Card-Not-Present (CNP) fraud between $25 billion to $40 billion[4].

Unfortunately, the solution is not as simple as just adding extra security measures. Research has shown that there is a fine balance to be achieved between customer security versus customer experience.

75% of businesses want robust authentication and security measures1 but that have little to zero impact on the digital customer experience.

Too many security measures and you risk alienating shoppers by adding friction to the shopping experience. Not enough security and customers become easy targets for online fraudsters.

It can be a tough balance to strike.

Up to 72% of consumers would transact more online if security measures were less obtrusive but, at the same time, 27% of shoppers abandon a transaction because there's not enough visible security[1].

We'll look at some of the more common authentication trends in online payments and how successful they are in providing sufficient anti-fraud protection, while maintaining that all-important balance between security and user experience.

3D SECURE 2

The original 3D Secure protocol (3DS1) was one of the first available online authentication measures. It provides a much needed additional security layer in CNP online payments and, because of its effectiveness, has enjoyed wide adoption since the release in early 2000.

It was identified as one of the top 5 tools against fraud used by businesses and by the end of 2017, 50% of merchants were expected to have implemented 3D Secure[5].

3DS2 is the second iteration of the 3D Secure protocol. It addresses many of the consumer and merchant related issues with 3DS1, most notably shopper abandonment rates and incompatibility with mobile devices.

A strong focus on the user experience and on security measures that can stand up against modern online fraud tactics, means 3DS2 provides for a smooth checkout experience without compromising on customer protection.

The technology has a number of unique features, which have helped it to evolve into one of the must-have anti-fraud tools in online payments.

3DS2 is the only issuer approved authentication method and allows for a liability shift of fraudulent chargebacks. This means, under certain conditions, if a fraudulent chargeback does occur, and the card issuing bank supports the 3DS protocol, the liability shifts from the merchant to the issuer.

3DS2 is also one of the only authentication tools that combine a number of standalone anti-fraud technologies, such as biometrics and One-Time Passwords, into a single, one-stop solution.

The original 3DS protocol relied upon an additional step during the checkout process that asked users to verify their identity by entering a static password. The concern for merchants was that the additional step added a lot of friction to the checkout process, causing customers to abandon the transaction. As a result, adoption rates in many regions were very low, including in the US.

With 3DS2 this will change. Enhanced information sharing between merchants and banks allows for the collection and analysis of additional contextual data related to a purchase, meaning the implementation of risk-based authentication is significantly more effective. So much so that Visa estimates that with the improvements in risk-based authentication, 95% of transactions would be classed as low-risk[6] and therefore go through the frictionless flow of 3DS2 with no additional customer verification needed (authentication is happening entirely in the background.)

BEHAVIOURAL ANALYTICS

Around 45% of merchants use customer website behaviour or pattern analysis software as part of their customer authentication strategy[5]. One of the more popular concepts is behavioural analytics.

Behavioural analytics allows merchants to identify potential fraudsters by learning the individual behaviours of their existing customers through the collection and analysis of thousands of unique data points during each return visit.

Companies can embed small snippets of code into a website or mobile application to automatically collect all the data points. This data can then be analysed to create a unique user profile for each customer that visits the eCommerce shop, based on their normal behaviour.

Behavioural analytics systems are designed to detect any abnormal or new behaviour from an existing client, determine how big the risk is of fraud is (i.e. how erratic is the behaviour) and then choose whether or not to intervene based on the level of risk.

What makes behavioural analytics effective in detecting and preventing online fraud is the real-time monitoring of all activities. It allows for an early-stage intervention, i.e. before a transaction is entered. Anomalies can be detected just by how a user interacts with the webpage, what they are clicking on and how fast they are moving from page to page.

A major issue with this type of authentication though is how unique the data points are that the system is collecting, and how accurately it can be used to create and eventually match to individual user identities.

If you take into consideration that, as humans, our online behaviour is not 100% consistent every time we interact with a site. We act differently depending on what time of day it is, if we are tired, rushed or perhaps even injured. This opens behavioural analytics to a big possibility of failure which can add even more friction to the customer experience, especially when an authorised user of an account is blocked from transacting and has to go through additional steps to unlock their account.

RISK-BASED AUTHENTICATION WITH BIG DATA AND MACHINE LEARNING

Risk-based authentication starts with the collection of massive volumes of information (known as big data) from users, such as the device being used, operating system, the IP address, time of day, transaction amount, etc.

Machine learning capabilities are then used to analyse this large dataset of information in real time and look for clues, anomalies, and discrepancies in the data to assign each transaction with a risk score.

Based on that risk score the system will then decide whether additional authentication is necessary or whether the risk is sufficiently low enough for the transaction to complete. The good thing about risk-based authentication is that the whole process happens in the background without the customer's knowledge, unless an additional authentication challenge is required. This means that the customer checkout experienced is significantly improved.

Factors that might inflate the risk score include using an unknown device from an unknown IP address or making an abnormally large purchase for multiple items.

Risk-based authenticating using a non-rule based, self-learning engine, i.e. machine learning, has been proven to be highly accurate and can result in more than a 90% reduction in fraud in some cases[7].

In a typical deployment, less than 6% of transactions require additional authentication (in the form of one-time passwords, biometric information, etc.) while around 2.5% of transactions are classified as high risk and blocked. Of the transactions that are blocked, only 58% required further investigation from the issuer and only 9% of those were actual genuine transactions by authorised users[7].

That means, statistically, the error rate for a machine learning, risk-based authentication engine, where an authentic purchase gets blocked in error, is only 1.3 transactions out of every 1,000.

The more transaction volume and data sets the system is exposed to, the more accurate it will get.

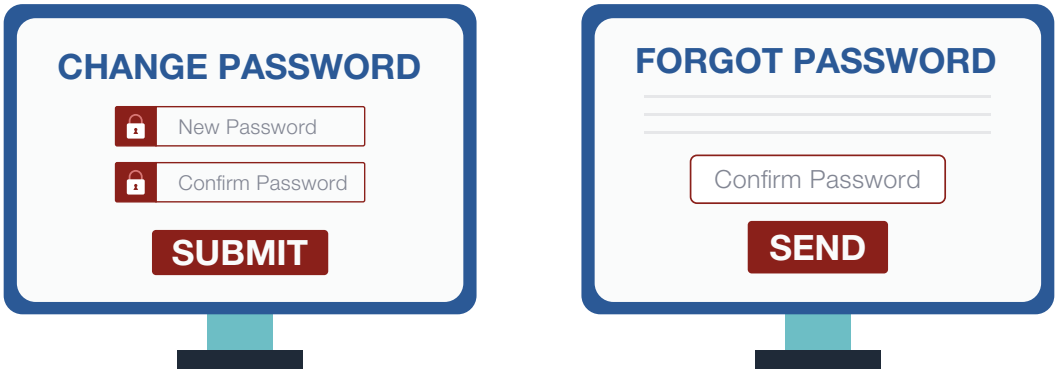
STATIC PASSWORDS

The password is the oldest authentication method and still the most popular. 52% of businesses rely on passwords as the top form of authentication[1].

Unfortunately, it's also the easiest for cybercriminals to steal from users and therefore, the least secure. 37% of consumers change their account passwords less than once a year and only 19% change it at the recommended time[1].
Many of us tend to use the same password for different accounts meaning that if a fraudster gets a hold of it, all of the various accounts are compromised.

Static passwords and usernames can also add additional friction during a transaction process as 25% of consumers forget their password or username within the first 6 months[1].

If we look at the balance between customer security versus customer experience, static passwords, although still widely used, are very ineffective.



ADDRESS VERIFICATION SYSTEM (AVS)

AVS is more of a fraud prevention measure than an authentication tool. It enables merchants to compare the billing address with the card address held by the issuer. When card details are captured during a transaction, the merchant can also require customers to enter their billing address. Once the transaction goes through, an AVS response code is sent to the merchant. This is simply a letter that corresponds to the verification provided.

Apart from a straightforward “exact match” or “no match”, there are around 18 possible response codes, each with a different meaning. “A” could mean the street address matches but the Zip does not, while “C” could mean the street address and postal code was entered in the wrong format.

It is then up to the merchant to either approve or decline the transaction, depending on how comfortable they feel with the AVS response.

There are a number of issues with this technology from a security and authentication standpoint.

It doesn’t verify the cardholder identity, only the address attached to it. If a fraudster manages to get a customer’s card details, the chances are high that they can also get their billing address.

While 77% of online merchants in the US have implemented AVS, it is not widely adopted outside the US and therefore not very useful for international payments[8].

Finally, it does not impact on whether a transaction is approved or not. It gives a result as to the accuracy of the address provided. The merchant must make the difficult decision, based on this information alone, whether to decline the transaction.

Case studies have shown that typically 75% of transactions will come through as an exact match, meaning merchants must make a decision on 25% of transactions and take on the liability if they make the wrong decision[8].

Again, it can also add additional friction to customers if they perhaps enter the correct address but not in the exact format as per the issuer records and the merchant decides to decline the transaction.

BIOMETRIC AUTHENTICATION

Biometric authentication, such as fingerprint scanning, retina scanning, speaker recognition and facial recognition, are regarded as the most effective standalone authentication method currently available because of how difficult it is to actually mimic or copy someone's biological features.

It works by simply scanning the unique features of a customer and comparing it to the records held in the account file.

It is very easy to use as most smartphones have built-in biometric capabilities such as fingerprint scanning. Biometric authentication also provides for a completely frictionless checkout process as no password, or username have to be remembered to prove a customer's identity. Online purchases and authentication can be done from the same application on the same device.

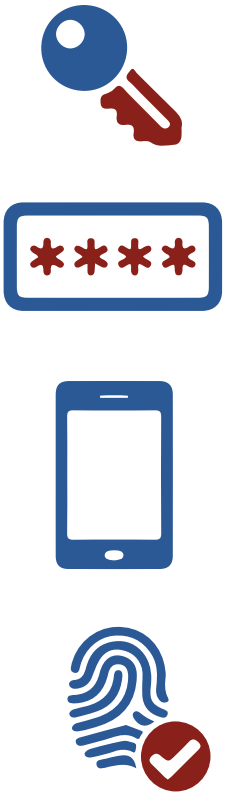
Biometrics is therefore the perfect solution to provide an enjoyable customer experience at a high level of security.

$30 BILLION

As such, the biometrics market is expected to grow into a $30 billion industry by 2021[10] with 93% of consumers preferring biometric authentication to passwords and 92% of banks stating they want to adopt biometric technologies[9].

MULTIFACTOR AUTHENTICATION

Multifactor authentication is a growing trend with 44% of businesses relying on it as their chosen method for customer authentication. It involves a process where more than one method of authentication is required, including some of the processes we discussed above, to verify a consumer's identity.



The methods of authentication used are based on three elements:

- Something that the user would know, i.e. knowledge check. An example of this is a password.
- Something that the user has, i.e. possession check. An example of this would be a one-time password sent to a mobile device.
- Something that the user is, i.e. identity check. An example of this would include biometrics.

Although using all three aspects in customer authentication is recommended for Strong Customer Authentication (SCA) according to certain regulations, such as the second Payment Services Directive (PSD2) in Europe, many businesses implement a Two-factor authentication (2FA) system where a user will typically have to confirm the knowledge and possession elements.

2FA is a very effective method of security but can be cumbersome for users, especially in a payments scenario, and can lead to increased cart-abandonment. 74% of businesses that use two-factor authentication receive complaints from users, with 9% saying they actually hate it[11].

This added friction to the user experience is perhaps why less than half of businesses have so far adopted the practice for customer authentication.

GEOLOCATION

Geolocation is a method of shopper identification that relies on determining the exact position of the transacting device to accurately authenticate the user.

If a user's registered address is in the US but the card is used in an attempted transaction in the UK, this transaction could very well be blocked by the issuer, unless the user called their bank in advance, informing them that they will be visiting the UK and might use the card during this time.

Most users have probably already come across this type of technology when using Google in a foreign country, for example, and the results are displayed in the native language of that country. A common way of in-browser location tracking is by using the IP address to determine the position of the device.

On mobile phones, the location identification can even be more accurate, by using cellular signals to triangulate the user's position or by leveraging the built-in GPS capabilities in smartphones.

Geolocation authentication is great from a customer experience standpoint as its very non-intrusive and top geolocation software report accuracy levels of between 97% and 99% on a country level[12].

The issue though is that this technology is very accurate at authenticating the device position, which in most instances can be an early fraud prevention tool, but it does not authenticate the actual user of the device.

Online IP addresses can be manipulated with VPN's and proxy browsers to mimic the registered address. And if merchants block purchases from proxy servers or VPNs as a rule, they risk losing sales from legitimate customers who are using these types of software because of growing concerns over online privacy.

CONCLUSION

There are a number of online authentication trends available to merchants today. However, very few of them get that delicate balance right between robust customer security and a frictionless user experience.

Most authentication technologies and software either provide a completely non-invasive authentication experience but one which could be easily manipulated by fraudsters, or very secure authentication systems but ones which come at the expense of the user experience, resulting in a decrease in conversion rates.

Furthermore, businesses want future-proof solutions that can keep up with regulatory requirements, such as Strong Customer Authentication under PSD2.

Finally, we live in an increasingly digitised world that has given rise to the now common term, Big Data. A typical transaction process will make a large amount of data available, which can be user-specific, product-specific or location-specific. Authentication systems need to be able to leverage this data without compromising user privacy. The more data points that can be processed and analysed, the more accurate the authentication engine will be and the higher the probability that it will be able to distinguish legitimate transactions from fraudulent ones.

If we consider all these individual points, the only technology that is suited to the task, by incorporating all these elements into a single, robust solution, is 3D Secure 2.

It provides an enhanced user experience through the application of risk-based authentication that allows for accurate user identification in the background.

It allows for more information sharing between merchants and issuers, meaning 3DS2 is now able to capture more contextual and richer data sets related to purchases, making the risk-based authentication and frictionless flow application even more accurate.

And in the rare cases that additional verification is necessary, the move away from static passwords to biometrics and token-based authentication not only provides increased security for users but also allows merchants to be regulatory compliant with SCA requirements.

Finally, 3D Secure is a recognised technology that is widely accepted. For merchants that already use 3DS1, simply updating to 3DS2 makes sense from both a cost-saving and time-saving perspective, on top of the unrivalled balance that it will provide in customer security versus customer experience.

Sources:

1. https://www.experian.com/assets/decision-analytics/reports/global-fraud-report-2018.pdf
2. https://www.invespcro.com/blog/global-online-retail-spending-statistics-and-trends/
3. https://www.experian.com/blogs/ask-experian/the-state-of-online-shopping-fraud/
4. https://financeandriskblog.accenture.com/cyber-risk/finance-and-risk/the-scope-of-the-card-not-present-cnp-fraud-problem
5. https://www.cybersource.com/content/dam/cybersource/2017_Fraud_Benchmark_Report.pdf
6. https://www.visaeurope.com/media/pdf/visa-infographic.pdf
7. https://globalrisk.mastercard.com/wp-content/uploads/2015/12/Advantages-of-Risk-Based-Authentication.pdf
8. http://www.fraudpractice.com/fl-avs.html
9. https://newsroom.mastercard.com/news-briefs/overcoming-mobile-biometric-challenges-mastercard-and-university-of-oxford-collaborate-on-new-research-initiative/
10. https://identity.utexas.edu/assets/uploads/publications/Current-Biometric-Adoption-and-Trends.pdf
11. https://www.esecurityplanet.com/network-security/74-percent-of-organizations-using-two-factor-authentication-face-user-complaints.html
12. https://www.cl.cam.ac.uk/~nz247/publications/JSAC2011-Geolocation.pdf