Since January 2020 Elsevier has created a COVID-19 resource centre with free information in English and Mandarin on the novel coronavirus COVID-19. The COVID-19 resource centre is hosted on Elsevier Connect, the company's public news and information website.

Elsevier hereby grants permission to make all its COVID-19-related research that is available on the COVID-19 resource centre - including this research content - immediately available in PubMed Central and other publicly funded repositories, such as the WHO COVID database with rights for unrestricted research re-use and analyses in any form or by any means with acknowledgement of the original source. These permissions are granted for free by Elsevier for as long as the COVID-19 resource centre remains active.
Why are SMS codes still the global ID solution?

Chris Stephens, Callsign

SMS one-time passwords (OTPs) have become the default ‘step-up’ authentication option when individuals are performing high-risk actions online. It’s because this approach is relatively easy for businesses to implement, and it works for most of their customers who nearly all possess a mobile phone and are familiar with OTPs. As a result, businesses typically use OTPs to authenticate both their customers and employees; and many banks are relying on this method to quickly comply with the upcoming PSD2 Strong Customer Authentication (SCA) regulation.

But given that the majority of organisations currently place their trust in SMS OTPs to authenticate their users and customers, it raises key questions: have we put all our (authentication) eggs in one basket? And with the deadline for SCA for e-commerce being extended to September 2021 due to Covid-19, does this present an opportunity for companies to look beyond SMS OTPs to more intelligent forms of authentication, including biometrics?

When it comes to SMS OTPs, banks and wider businesses should consider important factors they might have overlooked, such as their hidden costs and security vulnerabilities. In fact, Google recently announced that it is moving away from SMS OTP-based authentication. And in the UK, both the Financial Conduct Authority (FCA) and UK Finance have said that in the longer term, banks should be minimising their dependence on their use.

Criminal exploitation

One key problem with SMS as the go-to solution for authentication is that criminals recognise that organisations are highly reliant on them for 2FA (two-factor authentication) transactions. As a result, scammers continue to abuse and weaken the security systems in place, and exploit these methods for their own advantage.

Currently, fraudsters widely practise SIM-swap fraud – where they obtain personal information about the victim, then contact the target’s mobile operator and claim that their phone has been lost or stolen. Once the fraudster has gained the confidence of the mobile operator, a number transfer is authorised, and the number is activated on a new SIM card. In this way, the fraudster gets access to the victim’s number and is then able to access all the one-time passwords and authentication codes that are sent to the victim’s number.

This hacking threat comes at a time when customers are less willing or able to visit stores during the current coronavirus pandemic, which means operators are more reliant on online channels. The result is they are even more vulnerable to this type of manipulation as they service their customers.

Beware of scammers

But it is important to recognise that SIM-swap fraud is not the only method fraudsters can use to intercept OTPs from their victims, both during the current pandemic and in the longer term. Malware and remote access apps on mobile devices provide an additional opportunity for scammers to steal SMS OTPs.

For example, fraudsters are increasingly using social engineering to deceive individuals into downloading remote access apps, such as TeamViewer or hidden surveillance software. These apps either give fraudsters remote access to the victim’s device – allowing the criminal to directly read their messages – or silently record all the victim’s messages and phone calls and forward them to another device. Either way the individual’s private messages, including OTPs, are intercepted by the fraudster in the same way as with a SIM-swap attack. The difference in this case is they have direct access to the victim’s device, often without them knowing.

There are several parties involved in the delivery of OTPs, and each provides an opportunity for messages to be captured. Combine this with the underlying vulnerabilities in the global SS7 phone network, and the attack surface and potential for mass compromise is evident.
banks need to ensure they have a clear view of all their data sub-processors and that each has suitable security controls in place, such as multi-factor authentication (MFA), audit logs and dashboards. Likewise, all telephone numbers need to be auto-redact ed to reduce the impact of data breaches.

**Hidden costs**

In addition to the potential fraud losses that result from intercepted OTPs, there are other unforeseen costs that can stack up. Beyond the obvious charges for SMS OTPs, such as cost per text, there are a number of hidden overheads that are difficult to budget for. These costs are typically a by-product of the issues cited above – and strategically, this forces organisations into a reactive mode that is difficult to manage.

For example, where drop-offs occur in an authentication process, such as SMS texts not being received, banks will need to be prepared for a significant increase in incoming calls to their customer service helplines, and the associated costs. Or, worse for the bank, the customer takes another card out of their wallet. In addition, consumers may ultimately abandon transactions as they are pushed along a customer journey that simply adds too much unnecessary friction. These abandonments result in a drop in interchange fees for banks, and potentially a reduced customer base for merchants.

**Consider the user experience**

Another issue is that SMS is not a universal solution for all customers. For instance, SMS OTPs are not accessible to everyone, such as those living in remote or low-service locations, who may find it difficult to receive SMS alerts. Nor is the experience very customer-friendly. For example, it takes approximately 30 seconds of transaction time for the text to go through, as opposed to the almost instantaneous transactions that can be achieved with biometric authentication.

Mobile adoption is not going to slow down any time soon, and the volume of transactions taking place on these devices will inevitably rise. This comes hand in hand with ever-changing customer needs and expectations as users look for hyper-personalised online experiences. And while SMS OTPs are mobile-first, this approach requires the user to move to an alternate platform to complete the transaction. Understandably, this can be extremely frustrating for the customer. Such a friction-filled experience could lead to users abandoning transactions, in the worst-case scenario. For these reasons and the known security implications, the EBA is recommending banks look to alternative options.

For organisations to meet the requirements of their whole customer base is far from easy. With fraud risk and compliance to consider, alongside the user experience and costs, it is hard to find a middle ground. However, with the right level of visibility and control over authentication and authorisation processes, organisations can meet the needs of their entire customer base, without risking an increase in fraud or additional costs. A business-aligned decision engine that uses real-time contextual intelligence will help them to spot and prevent fraudulent activity before it can even take place.

**Using biometric authentication**

As industry becomes more aware of the negative aspects of SMS OTPs, the key challenges that most organisations face are to ensure they are using the right authentication factors for their customers, and that the user experience matches their brand. This focus on user experience also aligns with the FCA’s views on finding the right solutions for customers.

To balance out the high costs of SMS and offer an enhanced customer experience, banks should look to using intelligent authentication. This can be driven by a decision and orchestration engine that provides a range of more secure, dynamic and bespoke journeys for customers. Banks could also opt for passive forms of authentication, which leverage GPS, and biometric data and behavioural biometrics to verify a customer is really who they say they are.

For instance, to improve the user journey for customers carrying out online transactions, a bank could adopt behavioural biometric-based authentication which passively detects genuine behaviour in the background. This provides the bank with the assurance that the user is who they claim to be, and also offers customers a frictionless means to both authenticate and authorise transactions in one seamless action.

One method that achieves this is ‘behavioural swipe’. This builds on the fact that every individual possesses their own unique characteristics when swiping across their screen. This behaviour is identified through analysis of the data signals captured from hardware sensors when the user interacts with the device. These signals are used to derive user features such as finger movement, hand orientation and wrist strength. A combination of artificial intelligence and machine learning capabilities are then used to analyse this information to build up a unique model of that user’s swipe behaviour.

It only takes milliseconds to confirm whether the customer is genuine or a fraudster, allowing the bank to seamlessly carry out appropriate security actions. In this way behavioural biometrics is not only a good approach for positively identifying a specific customer, it also quickly identifies bad actors – for example, when fraudsters use technologies such as bots or remote access Trojans (RATs) to control transactional flows without the customer’s knowledge.

Behavioural technology works on both high and low-end devices and prevents a fraudster from using a victim’s device. This includes protecting against both blind attacks (where the scammer has never observed how the user swipes their phone) and over-the-shoulder attacks (where the fraudster has been able to observe the victim’s swipe movements). The algorithms used are able to detect both types of fraudulent attack, with an accuracy rate of 98%, while detecting the genuine user more than 90% of the time. This ability to prevent fraudulent access, even when the attacker has observed behaviour, adds a greater level of security that traditional methods, such as a PIN or password, cannot.

But no matter what behavioural biometrics approach a company chooses, it is essential that it addresses both the positive identification of the customer and bad actors committing fraud. This ensures that the solution
offers low margins for error, which minimises unnecessary fallbacks to less favourable authentication types.

Staying competitive

The most successful organisations, both during and after the current pandemic, will be those that are able to deliver hyper-personalised journeys – as consumers increasingly seek to bank with or sign-up to services that provide a bespoke service and meet their daily requirements and expectations. Yet, single-point solutions such as SMS OTPs offer little flexibility for organisations to meet these needs.

By investing in an intelligent authentication solution, banks will be able to significantly enhance the user experience and reduce IT costs by moving away from SMS OTPs and other knowledge-based methods. A recent survey by Callsign showed that in a single month, 20% of consumers switched to other brands due to a bad online shopping experience – such as failed payments, complicated log-in, etc. So it is crucial that banks and businesses remove customer pain points, improve service levels, and build trust with their existing customer base to achieve new ones.

By taking an holistic approach, organisations can take back control of their fraud and authentication management, offering staff greater intelligence around who the customer is, and the flexibility to amend customer journeys in real time. By taking this strategic outlook, they will be able to adopt a more proactive approach that provides more control and insights over where their budget should be allocated, while becoming less reliant on single-point solutions.

This not only enhances security measures, but also makes it difficult for fraudsters to identify the weak spots in an organisation’s network. A hyper-personalised approach, which uses intelligent biometric authentication, will improve the customer experience and Net Promoter Score (NPS) as users now have more choice and control over their own authentication journeys.

About the author

Chris Stephens is head of banking solutions at Callsign, helping clients to implement intelligent fraud and authentication solutions. He previously worked at Deloitte as a financial crime consultant and has a BA in mathematics from the University of Oxford. Callsign helps solve the challenges organisations face in getting their users onto and interacting with their digital platforms easily and securely. For more information, visit www.callsign.com.

References

1. Zak Doffman. ‘Goodbye SMS – Google Confirms Powerful New Update For Millions Of Users’. Forbes, 17 June 2020. Accessed August 2020. https://www.forbes.com/sites/zakdoffman/2020/06/17/google-confirms-powerful-new-security-move-impacting-all-users-goodbye-sms/#76bdd10b6c42.

2. ‘The SIM hijackers: how criminals are stealing millions by hijacking phone numbers’. Europol, 13 March 2020. Accessed August 2020. https://www.europol.europa.eu/newsroom/news/sim-highjackers-how-criminals-are-stealing-millions-highjacking-phone-numbers.

3. ‘Impact of 2020 Pandemic Report’. Callsign, 6 May 2020. Accessed August 2020. https://blog.callsign.com/impact-of-2020-pandemic-report.

Call centres: going voice-first in the post-Covid world

Michal Hrabí, Phonexia

The infamous first wave of Covid-19 has largely passed. Depending on the country concerned, the pandemic has been contained to some degree and many important lessons have been learned. Evidently, this global panic over such a tiny object travelling through the air has shaken old behaviours and long-established patterns, causing massive (transformative) changes in our society.

In economic terms, some companies have struggled with a severe fall in revenues, while others have been challenged by a sudden surge of incoming inquiries, calls and unexpected traffic. As a result, the scalability and security of organisations’ call centres, and their interaction with customers, has never been so tested as during this crisis.

Long-known issues

Of course, call centres have perennially struggled with scalability, even before Covid-19, and many of us have experienced this reality first-hand. Call queueing was considered as a normal part of the call centre experience. And even though cutting-edge voice automation technologies had been around for some time, there was never a serious need for an infrastructure upgrade. People were simply accustomed to the state of things and didn’t mind waiting sometimes.

However, the Covid-19 pandemic has put contact centres through serious heavy-load testing, uncovering the alarming impact that long call queues (especially on national emergency lines) can have during these challenging times. There is nothing worse, for example, than waiting in a phone queue caused by the massive wave of Covid-19 emergency calls, simply to be able to call an ambulance and fire fighters to a car accident.

Yet scalability is only one part of contact centres’ long-brewing issues. The other and equally challenging element has always been the verification of a person’s identity over the phone. Contact centres rely heavily on knowledge-based authentication (KBA), which demands a caller answers a set of security questions to prove their identity over the phone. Depending on the organisation’s security level, the person calling may even be required to answer a series of security questions in a row. And if any of the questions is answered wrongly, the authentication phase fails.

To preserve security, the person calling cannot receive hints to the question(s) they answered incorrectly – they have to hang up, call again, and try to get through the verification process once more. And as the questions are typically selected randomly from a wide set of pre-agreed answers, the customer can easily get some of them wrong. And if an unprecedented event happens – such as the global pandemic – this combination of limited scalability