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 NFC is a rising star in digital ID

Vikas Seth, IDnow

The Covid-19 pandemic has accelerated digital transformation across all industries, enabling many businesses to carry on trading while streamlining processes. But perhaps not surprisingly, this move to digital has been accompanied by a rise in cyber-crime and fraud. This in turn has accelerated the search for technology that can help improve the security of digital ID verification, while enhancing the experience for users.

Focusing on the UK market, government figures illustrate the scale of the challenge: they show that 39% of businesses suffered a cyber-security breach or attack in the 12 months to March this year1. Similarly, the City of London Police, the UK’s national force for combatting fraud, received nearly 4,000 reports of cyber-crime in the first month of Covid lockdown2, an increase of over 70% on the previous month and equating to £2.9 million in losses.

This massive spike in fraud, which began with the pandemic, reflects the increase in online activity worldwide by consumers as well as businesses. Without the freedom to pursue their usual in-person activities — such as domestic shopping, banking or signing up for a mortgage or loan — many people entered into new online territory that they simply were not prepared for.

Businesses too moved into unchartered waters. The constantly shifting situation around the pandemic provided an effective distraction for managers and employees, one that was compounded by the challenges of people working from home — again a new experience for many staff. These employees have largely been working using company laptops since the start of the first Covid lockdown, but some have not — exposing them to the security risks posed by using their own computer, alongside inadvertently downloaded malware, via a domestic router. It didn't help that some families were sharing equipment, with cyber-security the last thing on children's minds when they clicked on enticing links and downloaded games.

Equally, many organisations were confident about the security of their VPNs. Pre-Covid, business VPNs were mostly required just for occasional use, when unusual or emergency circumstances forced someone to work from home for a day. Nowadays, they are the mainstay of daily business life as remote and hybrid working patterns are becoming embedded. Cyber-criminals have recognised that this new, flexible way of working is here to stay and are finding increasingly sophisticated ways to hack into businesses dealing with consumers are under pressure to put ease-of-use and simplicity at the top of their priority list, with security an almost 'invisible' regard. Consumers want and expect an easy, seamless experience — and businesses have to be able to offer that or risk seeing those potential customers walk. This means any digital ID verification processes have to not only be robust, but also meet the preferences of customers with little patience for long-winded processes.

Again, not every customer is the same. Digital natives and millennials may be fine with some forms of digital onboarding, but older generations may find the idea genuinely off-putting. It's important to be able to offer a range of customer onboarding methods that have multi-generational and cross-demographic appeal. In order to increase conversion rates, a range of methods should therefore be available.

For example, video-based systems that involve a human agent may be preferable for some customers, as they are more like a traditional face-to-face meeting. And lockdowns ensured that even the more digitally-averse have become adept at Facetime calls with friends and family, making a live video communication an acceptable proposition for many who might have shied away from the idea before the pandemic struck in early 2020.

Onboarding new customers usually involves two main objectives — the authentication and confirmation of the presence of a valid identity document, and a second layer of security that confirms ‘liveness’. These checks remove the risks of a criminal using a stolen photograph or wearing a mask, an imposter or close look-alike.

The increase in online commerce conducted by businesses, consumers and government agencies since the start of the pandemic has inevitably included online banking and the sharing of sensitive financial information. Organisations have had to react to the Covid challenge and new ways of operating quickly and decisively, so it’s not entirely surprising that some mistakes were made and specific security checks were overlooked. State aid programmes, hastily put together to support individuals and businesses that were struggling, found themselves open to fraud. For example the UK Government’s Bounce Back Loans Scheme was targeted — and as much as £27 billion may have been lost to fraudsters and defaulted payments from this scheme alone3, alongside losses connected to other Covid-19 support programmes.

Again, some businesses were unable to weather the storm and others had to temporarily pause trading. This in turn meant many other companies were scrambling to identify new business partnerships — trading partners, suppliers and customers — almost overnight. The pressure to keep going meant that due diligence and KYC requirements weren’t always the top priority.

Improving ID verification

Against this background, business-to-business (B2B) identity verification systems broadly prioritise security over convenience: a certain amount of red tape is expected and accepted. But businesses dealing with consumers are under pressure to put ease-of-use and simplicity at the top of their priority list, with security an almost ‘invisible’ regard. Consumers want and expect an easy, seamless experience — and businesses have to be able to offer that or risk seeing those potential customers walk. This means any digital ID verification processes have to not only be robust, but also meet the preferences of customers with little patience for long-winded processes.

Against this background, business-to-business (B2B) identity verification systems broadly prioritise security over convenience: a certain amount of red tape is expected and accepted. But businesses dealing with consumers are under pressure to put ease-of-use and simplicity at the top of their priority list, with security an almost ‘invisible’ regard. Consumers want and expect an easy, seamless experience — and businesses have to be able to offer that or risk seeing those potential customers walk. This means any digital ID verification processes have to not only be robust, but also meet the preferences of customers with little patience for long-winded processes.

Again, not every customer is the same. Digital natives and millennials may be fine with some forms of digital onboarding, but older generations may find the idea genuinely off-putting. It’s important to be able to offer a range of customer onboarding methods that have multi-generational and cross-demographic appeal. In order to increase conversion rates, a range of methods should therefore be available.

For example, video-based systems that involve a human agent may be preferable for some customers, as they are more like a traditional face-to-face meeting. And lockdowns ensured that even the more digitally-averse have become adept at Facetime calls with friends and family, making a live video communication an acceptable proposition for many who might have shied away from the idea before the pandemic struck in early 2020.

Onboarding new customers usually involves two main objectives — the authentication and confirmation of the presence of a valid identity document, and a second layer of security that confirms ‘liveness’. These checks remove the risks of a criminal using a stolen photograph or wearing a mask, an imposter or close look-alike.

The Covid-19 pandemic has accelerated digital transformation across all industries, enabling many businesses to carry on trading while streamlining processes. But perhaps not surprisingly, this move to digital has been accompanied by a rise in cybercrime and fraud. This in turn has accelerated the search for technology that can help improve the security of digital ID verification, while enhancing the experience for users.

"NFC is a useful tool at a stage when it’s clear Covid-19 isn’t going away any time soon and biosecurity will continue to be a worry for many”

The increase in online commerce conducted by businesses, consumers and government agencies since the start of the pandemic has inevitably included online banking and the sharing of sensitive financial information. Organisations have had to react to the Covid challenge and new ways of operating quickly and decisively, so it’s not entirely surprising that some mistakes were made and specific security checks were overlooked. State aid programmes, hastily put together to support individuals and businesses that were struggling, found themselves open to fraud. For example the UK Government’s Bounce Back Loans Scheme was targeted — and as much as £27 billion may have been lost to fraudsters and defaulted payments from this scheme alone, alongside losses connected to other Covid-19 support programmes.

Again, some businesses were unable to weather the storm and others had to temporarily pause trading. This in turn meant many other companies were scrambling to identify new business partnerships — trading partners, suppliers and customers — almost overnight. The pressure to keep going meant that due diligence and KYC requirements weren’t always the top priority.

"NFC is a useful tool at a stage when it’s clear Covid-19 isn’t going away any time soon and biosecurity will continue to be a worry for many”

Focusing on the UK market, government figures illustrate the scale of the challenge: they show that 39% of businesses suffered a cyber-security breach or attack in the 12 months to March this year. Similarly, the City of London Police, the UK’s national force for combatting fraud, received nearly 4,000 reports of cyber-crime in the first month of Covid lockdown, an increase of over 70% on the previous month and equating to £2.9 million in losses.

This massive spike in fraud, which began with the pandemic, reflects the increase in online activity worldwide by consumers as well as businesses. Without the freedom to pursue their usual in-person activities — such as domestic shopping, banking or signing up for a mortgage or loan — many people entered into new online territory that they simply were not prepared for.

Businesses too moved into unchartered waters. The constantly shifting situation around the pandemic provided an effective distraction for managers and employees, one that was compounded by the challenges of people working from home — again a new experience for many staff. These employees have largely been working using company laptops since the start of the first Covid lockdown, but some have not — exposing them to the security risks posed by using their own computer, alongside inadvertently downloaded malware, via a domestic router. It didn't help that some families were sharing equipment, with cyber-security the last thing on children's minds when they clicked on enticing links and downloaded games.

Equally, many organisations were confident about the security of their VPNs. Pre-Covid, business VPNs were mostly required just for occasional use, when unusual or emergency circumstances forced someone to work from home for a day. Nowadays, they are the mainstay of daily business life as remote and hybrid working patterns are becoming embedded. Cyber-criminals have recognised that this new, flexible way of working is here to stay and are finding increasingly sophisticated ways to hack into businesses.
One solution that addresses these objectives, while also creating a seamless and straightforward user experience, is to combine NFC communications technology with video, fingerprint and ‘selfie’ biometrics.

“The biometric data that NFC chips hold is even more effective when used alongside other real-time digital sources, such as photo and video selfies”

NFC – or near field communication – works by using wireless communication, at a range of 4cm or less, to access a ‘passive’ unpowered device such as an NFC-chipped document or passport, that is temporarily powered by an active ‘reading’ device. It is now common technology, embraced by transport systems the world over, though first widely used in the UK back in 2003 by Transport for London (TfL) for its contactless Oyster Card. It’s the chip that enables passports to be read and checked instantly at airports, and the reason why contactless payment cards and mobile payment solutions like Apple Pay and Google Pay can access money with a simple wave in the direction of the payment reader.

NFC is a useful tool at a time when it’s clear that Covid-19 isn’t going away any time soon and biosecurity will continue to be a worry for many. NFC can help to contain the spread of the virus: its ‘tap-and-go’ process guarantees less physical interaction and provides a more hygienic way of operating than using government-issued ID documents. NFC technology also provides an additional layer of authentication, as ID retrieval is done from a digitised imprint on a chip. This is harder to manipulate than a paper document, so making it difficult for criminals to carry out ‘similarity’ fraud.

Today, the more up-to-date Apple and Android mobiles all have the ability to read NFC chips, making digital ID verification quicker and more secure. NFC chips hold biometric information about an individual that can be instantly compared with the in-person customer. It becomes even more effective when used alongside other real-time digital sources such as photo and video selfies to support remote onboarding. This blend of two secure processes protects the user experience, while securing their data and their digital identity from unwanted criminal interference.

NFC in Europe

Digital technology for improved ID verification is now becoming standard across Europe. And countries including Portugal, France, Germany, Switzerland and Austria are implementing law changes around NFC technology to enable digital ID verification. Currently, 14 European Union (EU) member states have their own national identity card systems, each designed independently in different ways with limited interoperability. In their place, the EU is introducing a ‘digital identity wallet’ where citizens across all member states can store their electronic ID (eID) such as driving licences, bank account details and even educational and professional qualifications. This will allow people to access online and offline services using their mobile phones, at home and across the trading bloc.

NFC is an added layer of security and compliance benefits alongside a user-friendly experience. France has launched a new digital identity service using an NFC ‘passport’. Citizens can use their smartphone to upload a selfie video. This captures their face from multiple angles with movement and expressions, which can then be compared to the photo in their biometric passport. This provides not only an accurate verification of the likeness, but also serves as a proof-of-life to thwart would-be ID theft.

The aim of this scheme is to offer secure identification authentication that will allow French citizens to access the government’s online services gateway. This is used by banks, other private sector companies and government agencies. Users simply have to complete a single registration that will then enable them to access multiple services.

As with all data transferred using NFC technology, images are not stored and cannot be copied, making them more secure. The verification video is deleted as soon as the ID is authenticated by the comparison with the biometric photo. This increased level of security also provides the user with more control over their own data.

“The EU is introducing a ‘digital identity wallet’ that allows people to access online and offline services using their mobile phones”

In Germany, meanwhile, national ID cards with an activated electronic ID function (eID) can be used alongside an NFC-enabled smartphone for more rapid digital identification.

Customer service

The key to customer satisfaction is to offer consumers the choice of an easy and inclusive experience, so that no matter how tech-savvy or tech-naive they are, there is a simple and hassle-free solution available for verifying their identity.

This type of increased control, combined with simplicity of interaction for the user, is the most persuasive argument for using a combination of NFC with other biometric identifiers. It gives those businesses that choose to deploy it a better chance of converting prospects into clients. And in competitive markets, it is important to offer processes that drive positive customer feedback, further supporting future conversion rates and bolstering reputation.

NFC used alongside mobile phone-based biometric identifiers is secure, compliant with legislation, protects personal data and is customisable for mobile and web integration. For customers there is no need for additional hardware. They can register their details at any time of day or night – using a system that works as easily as paying for their weekly shop with a phone or bank card.

Consumers can use the two technologies combined to register for services such as banking and other financial activities, insurance and telecommunications, within minutes.

There are also solutions available that use alternative additional verification methods, for customers who don’t have devices with the required eID or NFC-enabled specifications. Identity verification specialists can offer businesses a platform that uses digital verification via video-chat, backed by AI technology – or even using a customer’s existing and therefore authenticated bank account to send a refundable micro money transfer alongside a scanned ID document.
About the author

Vikas Seth is chief product officer at IDnow. He is an advocate of NFC technology, and is implementing this technology as part of the IDnow Platform to enable secure customer biometric verifications whilst combating fraud. Before joining IDnow, Vikas spent 20 years in product management at companies including Honeywell, EMC Data Storage Systems, AVG Technologies and lastly Avira, where he spent three years working as the director of product management and engineering.

References

1. ‘Cyber Security Breaches Survey 2021’. UK Government’s Department for Digital, Culture, Media & Sport, 24 March 2021. Accessed August 2021. https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2021.
2. ‘Cyber attacks increase as people work from home’. City of London Police, 9 September 2020. Accessed August 2021. https://www.cityoflondon.police.uk/news/city-of-london/news/2020/template4/press-releases/cyber-attacks-increase-as-people-work-from-home/.
3. ‘Taxpayers set to lose tens of billions in Government’s Covid-19 support schemes’. UK Parliament’s Public Accounts Committee, 30 June 2021. Accessed August 2021. https://committees.parliament.uk/committee/127/public-accounts-committee/news/156186/taxpayers-set-to-lose-tens-of-billions-in-governments-covid19-support-schemes/.

Calls for behavioural biometrics as bank fraud soars

Richard da Silva, Revelock

Behavioural biometrics – much like physical biometrics – is becoming an increasingly prevalent way for financial institutions worldwide to authenticate and verify their customers. At a time when a staggering 15 billion sets of stolen usernames and passwords – acquired through hundreds of thousands of data breaches – are circulating the dark web¹, behavioural biometric analysis promises to replace systems relying on personally identifiable information (PII) with a more secure and user-friendly alternative.

The most widespread use-case for this technology in financial services remains continuous user authentication. By capturing the way every user types, scrolls, clicks, swipes, zooms, touches their screen and even the way they hold their mobile device, behavioural systems give banks a unique and accurate digital ID for every person, known as their BionicID. If at any point during a user’s online banking journey their behaviour diverges from their usual or normal set of behaviours, this is flagged to the bank as a possible impersonation or manipulation attack, such as an account takeover by a bad actor or a bot. These attacks have been steadily rising in recent years and have become especially prevalent since the Covid-19 pandemic began.

Modern fraud tactics

During the pandemic, hackers have been able to prey on people’s feelings of uncertainty and anxiety over product scarcity, and revive tried-and-tested fraud tactics such as phishing attacks and malware. In particular, zero-day malware attacks – which aim to exploit new security vulnerabilities before financial institutions notice and create new cyber defences – have become especially common since banking became a digital-first experience during lockdowns and all customers were forced to get to grips with online channels.

To add to this, we are now witnessing the widespread ‘democratisation’ of fraud, where even non-technical fraudsters can more than double their investment through attack-as-a-service schemes. These techniques have lowered the bar for entry into the financial fraud ‘industry’, and almost daily we see new campaigns that use machine learning in some form to try to vary the attack vector.

With fraud methods constantly evolving, organised cyber-crime thriving, and more and more personal credentials making their way onto the dark web, online banking fraud has become a low-cost, high-reward enterprise for its perpetrators. Banks have historically been on the back foot when countering these attacks, with fraud losses amounting to £783.8 million in 2020 alone². Behavioural biometrics now promises to help shift the fraud strategies of financial institutions onto a more proactive footing, and help them stay ahead of emerging fraud tactics and zero-day malware.

¹ -london/news/2020/templa-4/press-releas-es/cyber-attacks-increase-as-people-work-from-home/.
² -london/news/2020/templa-4/press-releas-es/cyber-attacks-increase-as-people-work-from-home/.