White Paper

The future of identity

The future of digital IDs: better business and safer customers

The way we verify identity has evolved: it was passports and paper, then electronic data. Now, as technology accelerates, it is going digital. But, this latest move hasn't ironed out the main problem of costly, frustrating processes which people and businesses are faced when it comes to authenticating their identity.

What's coming next will make online life simpler and more efficient for everyone.

Too many passwords

The original purpose of the password was to secure an area – similar to locking the doors on your house or car, a preventative for people not permitted to access being able to enter. Banks, and other sectors such as ecommerce, all hold secure account information and the need for a user controlled access was mandated, resulting in the password.

The password has changed over time and offers a one-factor authentication. From simple passwords, to the use of complex characters. As a result of the widespread adoption of passwords, most customers transact through a series of websites using usernames and passwords to verify their identity. Using multiple sites means multiple IDs and passwords that are often difficult to remember. It's not uncommon for customers to need passwords reset or to go through a lengthy or difficult process of answering security questions, to prove who they are.

In addition, the customer is likely to have previously gone through a cumbersome set-up process to enable these kinds of digital based transactions. All of this time-consuming and annoying.

This can be just as frustrating for business too. At great cost, they provide a security infrastructure to manage username and password systems, helpdesks, and pay for staff to deal with queries and oversee the technology.

Given the time and annoyance experienced by the customer and the cost endured by businesses, the current system just doesn't seem sustainable. The future of identity will inevitably see a strategy that is efficient and customer-centric.

> "Passwords are yesterday's technology. They are both forgettable and vulnerable."

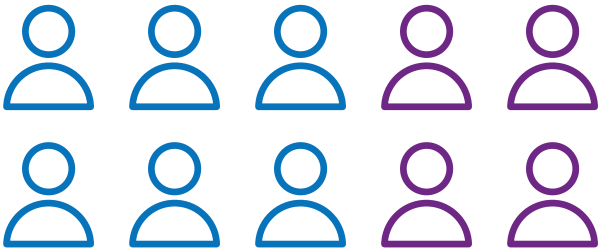
The average customer has **26 online accounts**

******

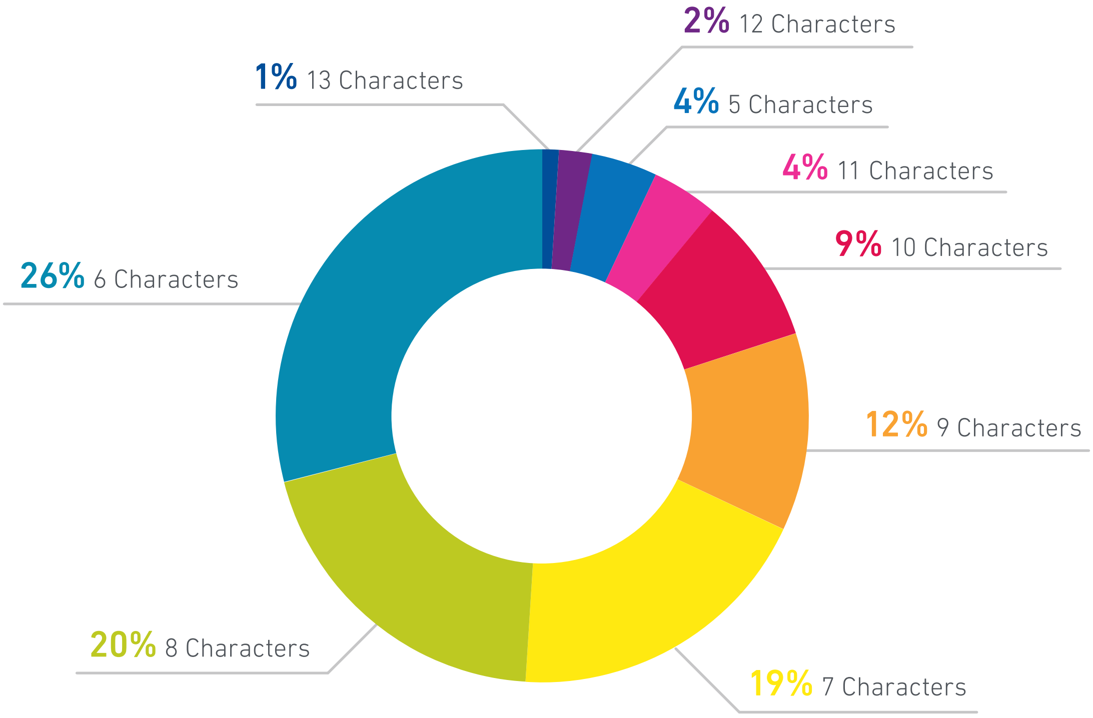
Most people have between 6 and 10 passwords they actively use

6 7 8 9 10

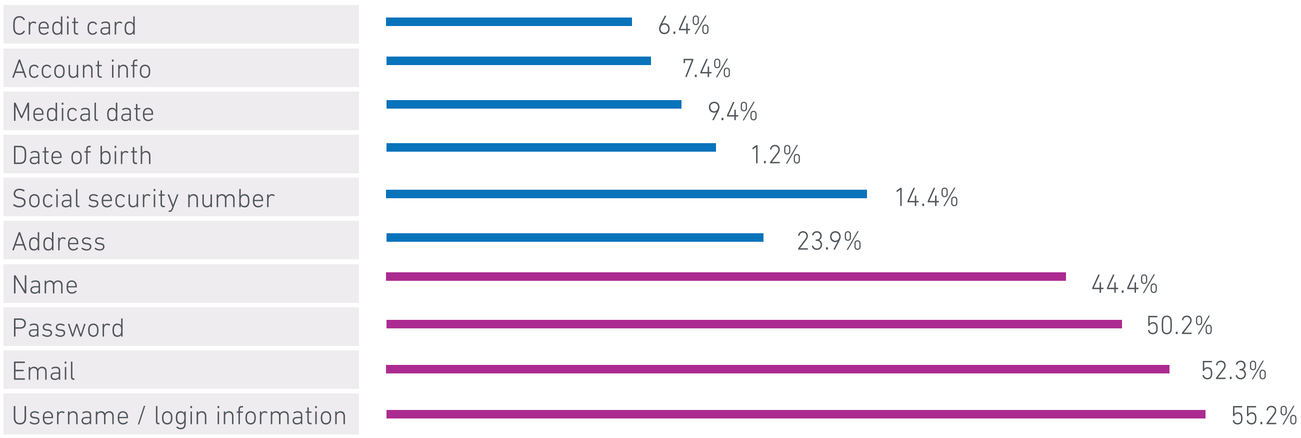
4 out of 10 need to use a password memory service to help them with remembering all of their passwords



8 characters is the recommended minimum (and should contain a mix of four different types of characters)



Passwords are targeted more than half of the time



Data targeted in 2012 breaches

Source: *Experian commissioned research, October 2016. **http://techinfo-4u.com/how-to-pick-a-rock-solid-password-infographic/

Will identity verification ever be able to truly cross borders?

Thanks to our mobilised, digital world, we're all connected. We're all transacting on a daily basis and as a result, we all need to be able to assert a verified identity.

To be able to continue to develop our globalised community, we all need viable digital 'passports' and the ability to verify IDs across borders. The European Union (EU) is already creating this digital single market.

The EU has already passed a regulation that sets out the rules of how this will work – eIDAS. It is underpinned by the fundamental belief that everyone should have the ability to prove their identity in both the online and offline world.

In November, the EU agreed the final stages of new laws to make online public services more efficient and more secure across the continent. It's part of a drive to make online cross-border interactions for citizens and businesses seamless, reliable and secure. To help this, Member States have agreed to set up a system that will allow people to use a digital identity verified in one country to access public services in other European states.

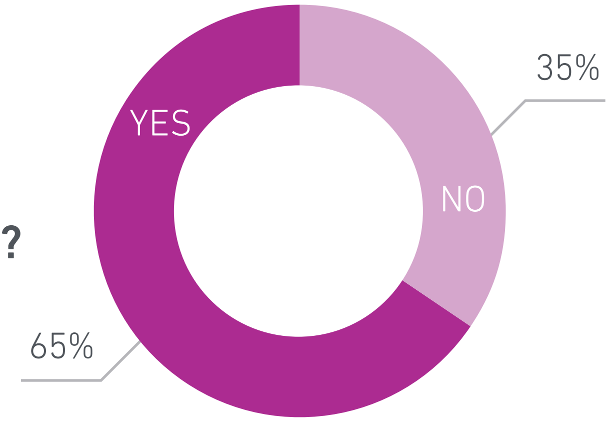
The objective is that a UK user may choose to verify their identity with their GOV.UK Verify account to prove they are who they say they are to the Danish tax authorities, making it easier to file your tax return should they live or work there.

Everyone should be included in the benefits that the digital world can bring in terms of speed of service, convenience and the ability to access the right, and best, services for every individual.

In time, the ability to verify an individual's identity anywhere on the globe will simply become a mandatory expectation. Right now we're still a very long way off from what's being predicted. As it stands the differing ID verification standards simply won't work together and irrespective of the concerns, it's a mission the EU is committed to.

"We're a long way off truly portable IDs, but the EU approach to a single digital market is a good step in the right direction."

Will ID verification ever be able to truly cross borders?



Not designed for trade

The internet wasn't originally designed as a trading platform. Given that most people now use it in this way that creates a problem.

The simple fact is: it all boils down to trust.

In the early days of the internet, it wasn't necessary to build-in ways to establish trust, but now that we all do business online those gaps are slowly being filled – and regulation is helping to drive this change.

Today, the internet see's over 3.6[1] billion global active internet users (2.2bn active social users, 3.7bn unique mobile users and 1.9bn active mobile social users). Nearly 88% of all adults in the UK have recently used the internet (in the last 3 months), which is 1.4% more than 2015 according to ONS. It is also growing (Internet users grew by 10% in 2016, up 354 million compared to 2015[2], and social usage grew 21% and mobile by 5%).

With the UK already making huge investments to combat cyber-crime and online fraud being referenced as the most common crime in the country (nearly 1 in 10 falling victim), it presents a growing threat.

"On the Internet, nobody knows you're a dog."

"Over 20 years ago the famous 'nobody knows you are a dog' cartoon was published. Somewhat ahead of its time then, it is of significant relevance today. With the rise of digital and a surge in cybercrime, understanding who your customers are, and validating their identity is essential."

[1] http://www.internetlivestats.com/internet-users/
[2] https://wearesocial.com/uk/blog/2017/01/digital-in-2017-global-overview

Owning identities

As more and more people become custodians of their own data, there is much more self-awareness toward identities.

With the proliferation of data, people are becoming more aware of their personal details and, in some areas, becoming much more astute to the risk of it being compromised. Equally, they are becoming savvier toward how their data can be a benefit to simplifying activities such as account access.

People expect their data to be used to enable much quicker, slicker and personalised opportunities from organisations – from prefilling data to easier validation. But, in a world ripe with cybercrime and a rise of 57%, between 2015 and 2016, in identity fraud[3], enabling the secure transfer of a person's data can be a complex challenge. Especially as most people believe it to be the responsibility of the business to protect and secure them from fraud. To overcome this a secure and robust process is essential and a shift in mind-set to individuals owning and protecting their own identity.

The implementation of a transferable digital identity will develop significantly in the future.

People and customers can retain control of their personal information and use this to their advantage in a way they feel comfortable. New opportunities like open banking will reaffirm this ownership to the individual and they could start to embrace the benefits that transferring a digital data set can give. Ease, speed, and accuracy will be the core component of a transferable identity – but accessibility will be the driving force behind adoption.

[3] According to CIFAS annual report

Should Government regulation shape the future of identity-based technology?

Widespread adoption and use of technology to help verify an individual's identity online could help customers and the digital businesses that serve them. But can regulation be the driving force to ensure security, usability, and access for all?

Online identity verification in the UK is already of an extremely high standard and is helping us drive down levels of digital fraud as a result.

This is the result of constructive and forward-thinking government standards defining the good practice. We only have to look at a few key characteristics of the current systems already in place in the UK to understand how regulation is a force for good.

The combined effect of regulatory demands – and the fact that regulations generally improve standards across the board, means the customer is protected. However, it's not uncommon for regulations to be formulated as a response.

With digital technology developing quickly and customer behaviour changing rapidly, regulations to drive up standards are likely to result in innovation to allow customer friendly compliance. Therefore, it comes down to the provider to establish best practice protocols and drive the development of industry-wide levels of consistent service and commonalities.

Organisations such as the Open Identity Exchange (OIX) are seeking to ensure standards across industry sectors are compatible enabling users to re-use one identity for many different only services.

For all the good intentions with which ID verification rules can be formulated, organisations can often become bogged down. No two customers are alike. An innovative verification system should be intuitive and versatile enough to cater for many different needs and expectations. The future is likely to see more regulation and more change. What will remain the same is the protection and focus on the customer. Those who can foster both areas to create a flexible inclusive solution will thrive.

"Government and industry need to work together to come up with standards that define the right level of identity assurance for each different online service."

Regulating identity

The growth in regulation has been a result of increased customer access and new market opportunities. With new markets in particular comes new risks, and businesses are currently striving toward finding solutions to restrictive compliance.

The Fourth Anti-money Laundering Directive (AML) is focused on growth and standardisation of Anti Money Laundering practices – aligned to the digital economy we live in today. Businesses who find and deliver elegant, robust and rapid due diligence to meet the criteria will be the ones who reap the benefits of this change.

The General Data Protection Regulation (GDPR) is another that promises to transform processes in order to standardise and protect data and the individual who owns it – therefore owning their identity.

Payment Services Directive 2 (PSD2) will enforce stronger customer authentication in order to initiate online payments. That could mean using a new generation of payment and authentication practice, such as fingerprint or facial recognition, as well as a new generation of security tokens and/or phrases. It will also mean varying levels of authentication for the customer – dependent on the transaction – and figuring out how to allow customers to transact on-the-go from a number of different devices.

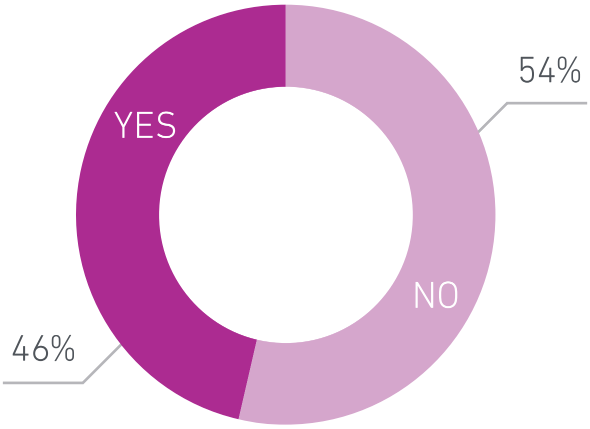
PSD2 will make it increasingly secure for customers to make monetary transactions and deal with financial providers across a range of devices. The challenge will be making this easier for the customer at the same time.

In the UK, the Digital Economy Bill will require age verification for certain online services.

These changes, and others like them, could lead us to a future where we'll all have secure, trustworthy digital identity that is transferable.

> "Regulation is rapidly catching up with the digital revolution. For a while it might get harder rather than easier to do business online."

Should Government regulation shape future identity technology?



Man vs. machine

As smart as technology is – the fraudster is smarter. This is where the omni-channel world causes a challenge for businesses who aren't considering the future. Typically, fraudsters will look for patterns and loopholes to ensure their criminal acts go undetected. As such, manual or rule-based software solutions will eventually be beatable.

As criminal capabilities grow more sophisticated, and penalties for non-compliance more immediately severe, businesses will need to consider a breadth of technologies that can support compliance and protect their business and customers. PSD2 defines acceptable fraud levels for low value transactions. Those who fail to meet these criteria receive more stringent regulated payments causing inconvenience for the consumer and the business.

Those who are able to implement effective fraud controls will reap the rewards of better customer experience and greater profitability.

Artificial Intelligence and Machine Learning are becoming more common as organisations seek to outsmart even the most sophisticated or emerging fraud trends. By 2020, 50% of developer teams will embed some level of cognitive services into solution development, saving in excess of £60bn, according to Deloitte. .

Shared advances in natural language processing and social awareness algorithms, coupled with an unprecedented availability of data, will soon allow smart digital assistants and bots to help with a vast range of tasks. From keeping track of your finances and health, to advising on suitable products and services.

> “Fraud controls that have been largely the same for decades are about revolutionised by the twin drivers of new regulation and innovations in technology."

Will the thumb replace the bank card?

Biometrics are being explored far beyond mobile account access.

A recent Experian-hosted debate focussed on whether a fingerprint could replace a bank card to obtain funds at a cash point. However, the consensus was that this would not be secure enough – because of the ATM itself. For example, the ATM could be tampered with and isn't a securely controlled piece of technology. But, despite the uncertainty seen from contributors from the debate, last month (April 2017), MasterCard released a biometric payment card that offers a multi-factor authentication - using fingerprint scanning to validate the user.

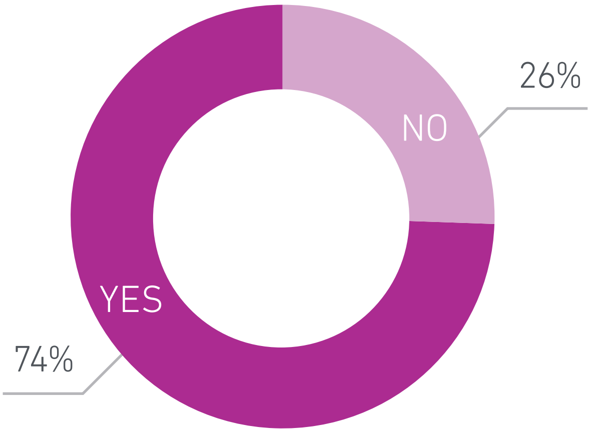
The MasterCard example is a big step toward the future direction and is a great example of how innovation will lead payments. The concept will likely change over the coming years but many believe will form part of a multi-factor approach – such as a fingerprint onto a phone, followed by contactless to an ATM to offer more security.

This also follows the multi-factor approach that PSD2 sets to mandate for card-not-present transactions and therefore a multi-factor concept is likely to emerge in the future – it just may not look like this example.

We have already seen a surge in payment transformations. From chip and pin to contactless and, more recently, phone and watch-enabled payments. This will continue to develop as the concept of a wearable, which is always on and always with you, summarises the digital society well. Technology is already here, although not yet widely available – or adopted, to its full potential.

> "While there will always be some people who prefer physical cards for payments, our panellists believe the move to broader use biometrics could be imminent and common by 2020."

Is biometric security the future of identity verification?



Identity inclusivity

Inclusiveness is critical and it's vital to ensure everyone is catered for equally.

Many segments of society are still dependent, or in favour of traditional means of identity validation and are likely to remain in favour of these methods for the foreseeable future. Their needs must be catered for. Equally some may be unable to access online systems due to disabilities, lack of confidence or knowledge. Therefore, relying on virtual authentication means far too many people will be excluded and a widespread adoption will be limited.

For the foreseeable future online only identities are unlikely to be truly inclusive, simply because there will always be a cohort that deliberately choose to opt out of using an alternative. But, some critics suggested chip and pin would never take off, but it did and has since become part of everyday transacting. As has contactless more recently.

“Online service providers will need to continue to cater for paper-based proofs being used by a minority for many years to come."

It is important to understand the differences of each individual and each customer segmentation. We explored how the Millennial and the Ageing Population differ:

	Millennial (18-34)	Ageing Population (55+)
Account Management		
Do you use the same bank for all of your credit and financial products?	Yes 50%	Yes 74%
Do you use your social media profile to access other accounts?	Yes 61%	Yes 24%
Do you have any paper-based accounts?	Yes 38%	Yes 58%
Have you walked away from an online application in the last 12 months?	Yes 59%	Yes 59%
If data was pre-populated for you, how would you find this?	Much easier to manage (29%)	Intrusive (51%)
How many passwords do you have across all accounts?	3	11+

Source: Research commissioned by Experian, October 2016

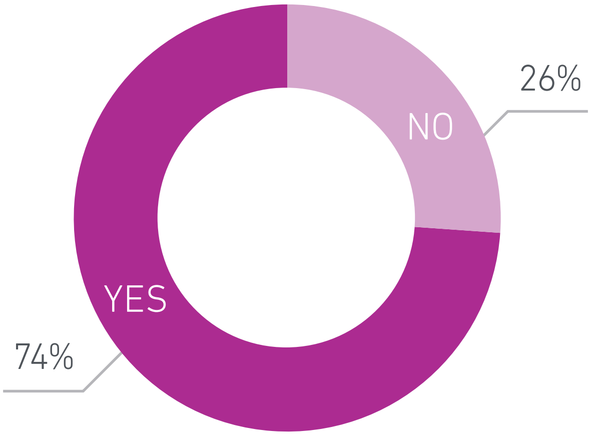
Behavioural biometrics

Behavioural biometrics is a developing technology and could be a new way to track and detect fraud attempts.

Rather than authenticating users this creates a tracking approach to detect suspicious activity. Passive, continuous behavioural monitoring could provide a new layer of security during and after someone logs in. This kind of 'multi-layering' of security and anti-fraud steps could work well with existing measures and other forms of biometric security in the future.

> "You are unique - even how you type and move a mouse is unique and difficult to copy."

Will technology help safeguard our virtual identities?



Smart technology is transforming how individuals can be identified

Biometrics, fingerprints, voice analysis, iris patterns, vein matching, gait analysis and more, are unique individual traits – and generally – difficult to fake. With the right technology, biometrics is likely to offer speed and scale to unlock the value in digital customer journeys.

There's a degree of unease around hyper-connectivity and personal privacy. But, with the right restrictions, well informed guidance and secure storage, safety shouldn't be hindered. Technology offers us some fantastic opportunities and businesses should continue to embrace them.

Irrespective of how 'smart' the technology is, there will always be concerns and counter-arguments suggesting the data underpinning it can be fraudulent, causing security issues. We're in a technological arms race with fraudsters and identity thieves. It's fair to argue that it will, in time, become as vulnerable as other platforms.

Smart technology and biometrics will be best used as an additional layer to security. It may not be for everyone but it's another tier of protection against identity theft. Likewise, some people may not be comfortable wearing devices – and what would happen in the event it was stolen?

Widespread adoption for virtual identities will see the issue of personal liability become a legal minefield.

As adoption and reliance on technology increase, it is certain the future will see even more debates around liability emerging as a result. The end outcome can't be predicted.

"We are at the dawn of a biometric revolution. Assuming all biometrics broadly difficult to spoof, the most likely biometrics to prevail are those that are easiest presented."

The changing fraud landscape

The demands of PSD2 ask that payments service providers put in a prescribed set of fraud controls in order to meet fraud thresholds. This will mean there is a consistent threshold across controls, but done in different ways. It will make the counter fraud measures used at the point of transaction broader and more sophisticated as payments service providers strive to keep below the fraud threshold of PSD2.

From a fraudsters' perspective, the introduction of biometrics will mean they will devise new methods that are designed to capture, reproduce or emulate biometrics. That won't be impossible to do, but will be much harder than traditional fraud.

Opportunist fraud, involving password capture, will be eradicated. The introduction of strong second factors will mean that fraudsters rethink how they attack.

Establishing an identity using someone else's details is likely to become the fraudsters' favourite approach rather than taking over any existing accounts. This means fraud controls at the point of account opening need to be as robust as possible.

Conclusion

New digital identities

Soon, an individual won't need to create endless profiles on each of the websites they visit.

Nor will they be required to establish their identity, to a high-level of verification, each time they want to engage with a business or website. Also, the retailers, insurers, banks, and other financial services they deal with won't need to invest in people, processes, and technology to run their identification systems.

We're nearly at the point where independent trusted identity providers, such as Experian, will work with individuals to create a very secure, single online profile that can be ported from website to website and used as a trusted way to verify their identity and perform transactions.

Biometric digital identity: A simple system for all

For the individual, this means not having to remember endless passwords, or spend time verifying their identity through a secondary route, or repeatedly entering their details to enable purchases.

For businesses, this simplified system means transactions will be immediate. Rates of abandonment caused by lengthy processes or forgotten passwords will fall, and customer satisfaction will rise.

Perhaps more importantly for businesses, they'll be relieved of the costs and operational burden of having to administer and maintain their own password and identification systems.

The future is moving in line with customers. As individuals take more control of their data, their identity profile will naturally form part of this; a single identity that can be used in many places, easily, securely and compliantly.

> "Log-ins, transactions, and identity verification will be seamless and instant – and, more importantly, much safer than ever before."

About Experian

Experian unlocks the power of data to create opportunities for consumers, businesses and society. At life's big moments – from buying a home or car, to sending a child to college, to growing a business exponentially by connecting it with new customers – we empower consumers and our clients to manage their data with confidence so they can maximise every opportunity.

We gather, analyse and process data in ways others can't. We help individuals take financial control and access financial services, businesses make smarter decision and thrive, lenders lend more responsibly, and organizations prevent identity fraud and crime.

About the author

Nick Mothershaw
Director of Identity and Fraud

LinkedIn connect with me

Nick is responsible for the strategic development of Experian's fraud and identity solutions.

The Identity solutions' portfolio includes electronic ID validation and ID verification through challenge questions, or document verification. Experian now offers a full Identity as a service solution, including ID proofing and strong credential management, and are one of the consumer identity providers within the GOV.UK/Verify scheme.

Fraud solutions in the portfolio include Device Fraud (FraudNet) and Application Fraud (Detect and Hunter). Key to the role is to ensure clients gain maximum value from our solutions by offering highly skilled consultancy services, expert analytics, trend analysis and insight around our fraud products, fitting our solutions to client's specific needs.

Nick has been with Experian for more than 12 years. Previously Nick was a director of a company providing global solutions within the broader criminal justice arena. Here, he developed the Scottish Intelligence Database – the only cross-force intelligence-sharing and matching solution in the UK.

Stay up to date with our latest fraud resources

- **Identity and fraud resource centre**
  – containing thought leadership and white papers covering topical fraud and identity related content

- **Latest thinking blog**
  – updated regularly exploring trends and topical insight around fraud and identity

- **#Fraudstats**
  – looking at trends and analysis from fraud by type

- **#FraudMap**
  – exploring regional trends of fraud

All statistics included within this document, unless sourced, are extracts from research commissioned by Experian. This includes consumer attitudes and appetite, October 2016 and Identity Debates, 2016.

Registered office address:
The Sir John Peace Building, Experian Way,
NG2 Business Park, Nottingham, NG80 1ZZ

T: 0844 4815 888
E: gtmcontactus@experian.com
www.experian.co.uk/identity