The evolution of digital identities
The evolution of identity
For many of us, the first time we gained an official identity was with a passport, driver’s licence, or other paper based document.

Over the last 20 years, paper has evolved to electronic data and paper documents are used less often in the verification process. This change has stemmed from organisations, like Credit Reference Agencies such as Experian, who can validate an identity using trusted data.

This system has served us well, but now it has run its course and is no longer inclusive of today’s needs and expectations. We are now a digital age and, consequently, identity verification must enter it too.

"Identity is on the cusp of a great change"
The evolution of digital identities

Identity has evolved. The rise of digital adoption from society and mobile usage, and the introduction of new authentication regulations have all contributed toward this change. In a data driven, hyper-connected world ‘identity’ has been a focus for many businesses, governments and regulators.

What does an evolved identity look like, and what has it become?

The surge of omni-channel customers and hyper-connectivity has changed the way customers and businesses interact and how products and services are delivered. The pace of change is accelerating all the time and increasing because of rising mobile use – giving online accessibility anytime, anywhere. Organisations create omni-channel journeys which take people on and offline. This can then cause friction when an identity is passed across channels.

An identity should be transferable, a footprint that is unique to the individual that they can use to validate and authenticate themselves, and is formed of multiple components. The fundamentals haven’t changed. What has however is the way in which people can translate and demonstrate their identity to validate, authenticate and authorise. This paper explores the transition from paper to digital, from passwords to biometrics, considering where we have come from and where we are today.

The next five years are likely to bring unprecedented change to the way the public establishes and verifies its identity online. Biometric information and social media accounts could become the bedrock of our personal digital identity.

So, how will that change work for the customer and businesses?
How people see the future of identity
We conducted a series of surveys to understand what people thought about the future of identity, and in particular certain elements such as regulation and biometrics.

Identity is evolving and digital, transferable identities that are shaped by regulation and technology, such as biometrics, is a likely development. This change is driven by a digital era that is fueled by data and convenience.
Are physical documents defunct?

Some say that the drive to introducing a digital identity could leave physical documents obsolete.

In today’s digital world, we still haven’t adopted an entirely paperless society. Transactions and accounts are opened online yet more than half (51%) of people keep paper based accounts, particularly females older than 55. Businesses start to engage customers’ digitally, for example using online applications, but then command paper-contracts and offline validation – for example when applying for a mortgage.

We are making headway and digital signatures are more common, as are digital receipts for retail and the elimination of physical car tax discs.

There are still a wide range of key documents including birth or death certificates, passports for example, which are necessary to keep as physical documents. And whilst we are fully immersed in a digital age, not everyone can be authenticated electronically as there isn’t enough known data about them. Therefore, there must be an alternative way to prove their identity to avoid them being excluded.

This is also essential for businesses as regulations stipulate they need to ensure an identity is proven. Some debate that online identities can be faked in the same way paper based copies can. However, as we move toward chipped and biometric documents it gives the balance of both.

A key development will be the creation of trusted digital identities based on the presentation of a mixture of document and electronic based evidence. The GOV.UK/Verify solution is a first adopter of this approach.

For the foreseeable future, the need for physical documents will remain. However, organisations need to consider how they blend digital and physical ID to support everyone’s preferences – compliantly.

Moving forward digital IDs will also present a cost saving opportunity through automation. It will also appeal more to the customer and enhance the customer experience.

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

Are physical documents defunct?

41% YES

59% NO
We asked people about what they thought about their finances in the future. This is what they said:

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

Identity theft is now a widespread problem that’s growing year on year, particularly around current accounts, where it has undergone a surge to record levels in recent years.

For today’s customer, identity theft can be a painful experience. Normally, they’re unaware of a theft taking place and only find out later that goods have been purchased in their name or a bank account has been falsely established using their details.

Unfortunately, when this happens it’s often down to the customer to prove they weren’t responsible.

Although providers are usually willing to accept that fraud has taken place, it can still be difficult to undo the mess they have been left with. It can take hours, even days, to have their credit history and identity rectified.

For businesses, identity theft means losses. If a false identity is used to obtain goods or services, a business is unlikely to have any other option than writing this off as a bad debt.

Greater assurance that a customer is who they claim to be will create confidence across the business community and reduce the prospect that fraudulent activity could leave a bad footprint on an otherwise genuine individual’s identity profile.
Will social data revolutionise identity verification?

Social media has made one of the most incremental changes to data and virtual identities this past decade. Are we on the cusp of a social identity revolution or does social media still lack the desired credibility?

As the Internet gains another 225 million active users around the world, social media growth is set to continue. In We are Social’s latest figure report on digital, social and mobile media usage around the world, social has seen an 8.7%* increase in just over eight months.

Usage of social media is most prevalent between the ages of 18 and 34 and most groups who use social media are all concerned with trust, privacy and security – but are swayed by the ease of use with nearly half of survey respondents using social media to register, or access, third party sites – suggesting that whilst concerned, it isn’t enough to prevent them using it.

The very nature of social media means that every interaction has a meaning. This can then be used to understand behaviours and contribute towards a profile – mainly by insight from the data social media generates.

Social data is complex, it’s layered and built up over time – and it’s hard to recreate that level of profile in such a short timeframe. It offers a wealth of different elements that together represents an individual – creating a unique user profile.

There’s a need to consider using social media for ID verification simply to meet customer expectations, offer inclusivity, match their current experiences and also ensure we reach the vast majority.

Social media data can enable an extra layer of validation for a user. But, it can also hinder a view due to the breadth of data it generates. This is why it is important organisations understand the data social provides and interprets it at a customer level.

Most social accounts were set up some time ago, and may not reflect accurate, current profiles – or have been set up correctly at point of account opening. For example, Millennials may have entered the wrong date of birth due to age restrictions, or others may have entered dormant email accounts or details as a means to not be hounded by marketing teams who access their data profile.

It’s very unlikely social data will be suitable as a uniform route to identity verification. It will undoubtedly add value to maintaining a single customer view however. The challenge is that when you create a social identity there is no upfront verification of who you are. Consistent social behaviour, over a long time period, is required to give the social identity credibility.

Another problem is account takeover – most social identities only use password for access, and are typically left logged on through devices for the users’ convenience. If they are easy to take over – can they be relied upon as good quality identity proofs?

The process of logging on to an account through a third party is something that will probably become a reality in the future. It is has already been adopted by ecommerce. For secure accounts however, this concept is likely to be developed even further due to concerns over privacy and security with social accounts. The concept, is something which will continue to play a part in a persons ability to identify themselves. With social media usage reportedly going to decline in the next decade, it raises a question about whether this will even be available to consider in five to ten year’s time.

As personal liability is questioned, and more ownership is given to the individual on their data, people will start to change their attitudes and start to protect their data much more. It wouldn’t be unreasonable to predict that individuals would use a trusted third party to help them do this.

“Whilst social media identities have mass adoption, the lack of due diligence in establishing the ID limits where they can re realistically re-used.”
Passwords
The path to establishing thorough and trusted digital identities hasn’t been faultless. As a digital economy, we’re still reliant on usernames, passwords, and security questions as a way to identify an individual.

Customers have become used to this type of data exchange in order to validate their identity when necessary. But, the fraudster has become all too familiar too.

Passwords are easy to forget. Research shows that most people have between 6 and 10 passwords they actively use, and 4 out of 10, need to use a password memory service to help them with remembering. With more than half changing their password when prompted, you can start to see a trend that suggests inconvenience. Interestingly, research also shows that people don’t think that retail, utility or social media passwords should be as secure as a bank. Even though a lot of these hold bank details and personally identifiable information. (44% on average think they should have a very secure password, compared to 86% who think a bank password should be very secure).

These are often used in multiple accounts, including using the same password for a bank account as they do a retailer. This represents a fraud risk. The many advantages offered through new and sophisticated technologies, are not being fully utilised – but all that is about to change.

“Passwords are yesterday’s technology. They are forgettable and subject to compromise.”

The average consumer 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).

- 1% 13 Characters
- 2% 12 Characters
- 4% 11 Characters
- 4% 10 Characters
- 9% 9 Characters
- 12% 8 Characters
- 26% 6 Characters
- 20% 8 Characters

How many passwords do you use?

- 0%
- 5%
- 10%
- 15%
- 20%
- 25%
- 30%

Age group of respondents:
- 18-24
- 25-34
- 35-54
- 55-64
- 65+

The evolution of digital identities | Page 11
Biometrics
Its likely passwords and usernames will be replaced. Or at least augmented with some form of biometric login.

Headway has already been made and many banks allow access by fingerprint to view account information and engage with their accounts. And more recently voice.

Because biometric information represents who an individual is. A fingerprint, an impression of an iris, a voice or a face, are things that a people can’t forget or lose, and are resilient against fraud.

“Biometrics are today’s technology. They are more secure and you can’t forget them. Technology has got to the stage where their mass use is now a reality”

Is biometric security the future of identity verification?

<table>
<thead>
<tr>
<th>YES</th>
<th>74%</th>
</tr>
</thead>
<tbody>
<tr>
<td>NO</td>
<td>26%</td>
</tr>
</tbody>
</table>
Privacy and biometrics

Three in five people (61%) believe biometric identification is just as secure, or even more secure, than the current system of passwords – including anything from emails and social media, to banking and pension log-ins.

Some people have concerns over privacy – and want clear guidelines around responsible use, and as the concept of biometrics develops, it will be a necessity.

In a recent Experian hosted debate, some respondents had fears about biometric privacy whilst others had concerns over other data sources. For example, DNA profiling which gives away more about an individual than data points alone.

In addition, less than one in five (19%) people stated they are willing to have their ID verified in this way. Similarly, less than one in ten (9%) would be comfortable with camera facial recognition as a form of identification, while just one in twenty (5%) say they’d be happy using voice recognition technology to unlock their online accounts.

Willingness to adopt biometrics is increasing as they are already becoming a factor in everyday life, spearheaded by the inclusion of fingerprint scanners on newer smartphone models. Fingerprint scanning is the most comfortable area with nearly half (40%), saying they would be happy relying on it – and a large part of society is already using it. This perception however may be a result of it being a ‘tried and tested’ method – as fingerprint scanning is a common access tool already – even if it is in its infancy of use.

In the future, biometric data will form part of an individual’s personally identifiable information. This will have social repercussions as people are likely to attach more emotion to this type of data.

Organisations storing biometric data will need to meet robust security standards similar to those already placed upon the payment card industry today. The best route to using biometrics is to add it to the identity and fraud armoury, making it another element in a multi-layered strategy.

“Right now people are still wary of biometrics: Does it give too much away? But people are voting with their fingers – millions are already using fingerprint to secure their phones.”

---

Do you think biometrics are as secure as the current system of passwords?

- **YES**: 71%
- **NO**: 29%
Fraudsters and criminals will also try and find the easiest route in to commit an act of fraud. As a result, those organisations without advanced security and access technology are at the most risk. In contrary to voice, research shows that fingerprint scanning is a biometric identification that most UK adults are comfortable with – and 40% stated they would feel happy relying on this as a means of accessing their accounts. With less than 1 in 5 keen on retinal scans and less than 1 in 10 comfortable with camera facial recognition. Perhaps the majority of people feel these means are more intrusive?

*Research conducted by Opinium Research between 23 and 25 September 2015 among 2002 respondents to a nationally-representative sample*
Establishing trust
The next phase of development will see individuals establish a single, highly trusted digital identity with a provider such as Experian that can be used again and again for instant logs-in and transactions with apps and websites.

However, to do this people must have the confidence to share their data. Customer perception is that banks are generally very secure, in comparison to other industries such as insurers or utility providers. This puts established providers at a distinct advantage – however provides an opportunity for other industries to develop and adopt the principles that banks have enabled for decades.

Organisations that succeed will be those that can gain the confidence and trust of their customers, encouraging them to share their data in return for better value services that are not only secure but easy for them to consume.

When you look at the depths of trust and perception of fraud, many people assume it to be the responsibility of the business to protect them. As such, it is imperative any organisation who offers any form of process that requires a transfer of data or capture of personal information, must act responsibly. This shouldn’t mean hindering innovation or new concepts of identity verification, but should do with caution and with the customer at the forefront of any development.

Organisations are already moving toward customer focussed teams enhancing and creating processes and this will continue moving forward. Equally, working together and linking data from across organisations can enhance this even more.

“One identity used everywhere with confidence will be the norm, fairly soon.”
Identity inclusivity
The evolution of identity has excluded some people because of the reliance on electronic data.

Some organisations are starting to make headway within an inclusive strategy for identity verification through the introduction of new technology such as document scanning. While this is a positive measure, there is still more to be done. With online usage being the main driver behind developments within identity checking, it is dominating processes and innovations.

With both the United Nations and World Bank committed to providing digital IDs to every person on the planet by 2030, it is paving the way for future developments. Clearly it’s a very ambitious 15-year undertaking – but possible given the proliferation of mobile devices during the past 15 years.

But, many segments of society are still dependent on traditional means of identity validation and are likely to be for the foreseeable future. Therefore, virtual authentication means organisations may exclude far too many people. In fact, it’s fair to say even missing one person, is one too many.

In our debate people outlined how the future may see a forced change of direction. A few years ago you could book a budget airfare by phone. Now, with some airlines, it is online only. But, in this business model the organisation can choose who its customers are. When we look at a verification strategy for necessary access – it opens a whole new level of consideration and becomes a national strategy, rather than a choice over demographic customer groups.

What is certain is that organisations need to consider inclusivity at every touch point. Who will a new direction affect, and how can they accommodate those people? This may be a case of moving people in one direction through education, but however it is done, it requires a united move.

Inclusiveness is critical and it’s vital to ensure everyone is catered for equally. The most important thing is businesses start to consider what inclusivity looks like and puts the customer at the heart of any development.

“Identity providers need to find ways to get as many people as possible online, even if that means using paper proofs to establish a Digital Identity. In Europe this is the standard way of operation.”

Can online identity ever be truly inclusive?

43% NO

57% YES
Beyond biometrics:
We’re in the middle of a period of rapid evolution. We’ve gone from paper to electronic to digital and are quickly moving to biometrics that will facilitate instant, seamless access to all our favourite digital services.

While biometrics will be central to the next developmental phase of digital identities, social media networks could also play a significant role.

Billions of customers are already signed-up as users of the major social networks and many of them use their log-in, in varying ways, to identify themselves to other online service providers. The concept of re-using an identity created in one place, in another place is well established.

What is needed is trusted re-usable accounts, to open up instant access to higher risk, and/or higher value online transactions.

Adding a layer of trust to pre-existing accounts could be one way for robust anti-fraud and identity verification measures to become quickly and easily available to many.

Whichever methods come to dominate the way we will verify our identity, the systems must ensure enhanced usability, improved security, and reduce the reliance on multiple usernames and passwords.
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 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.