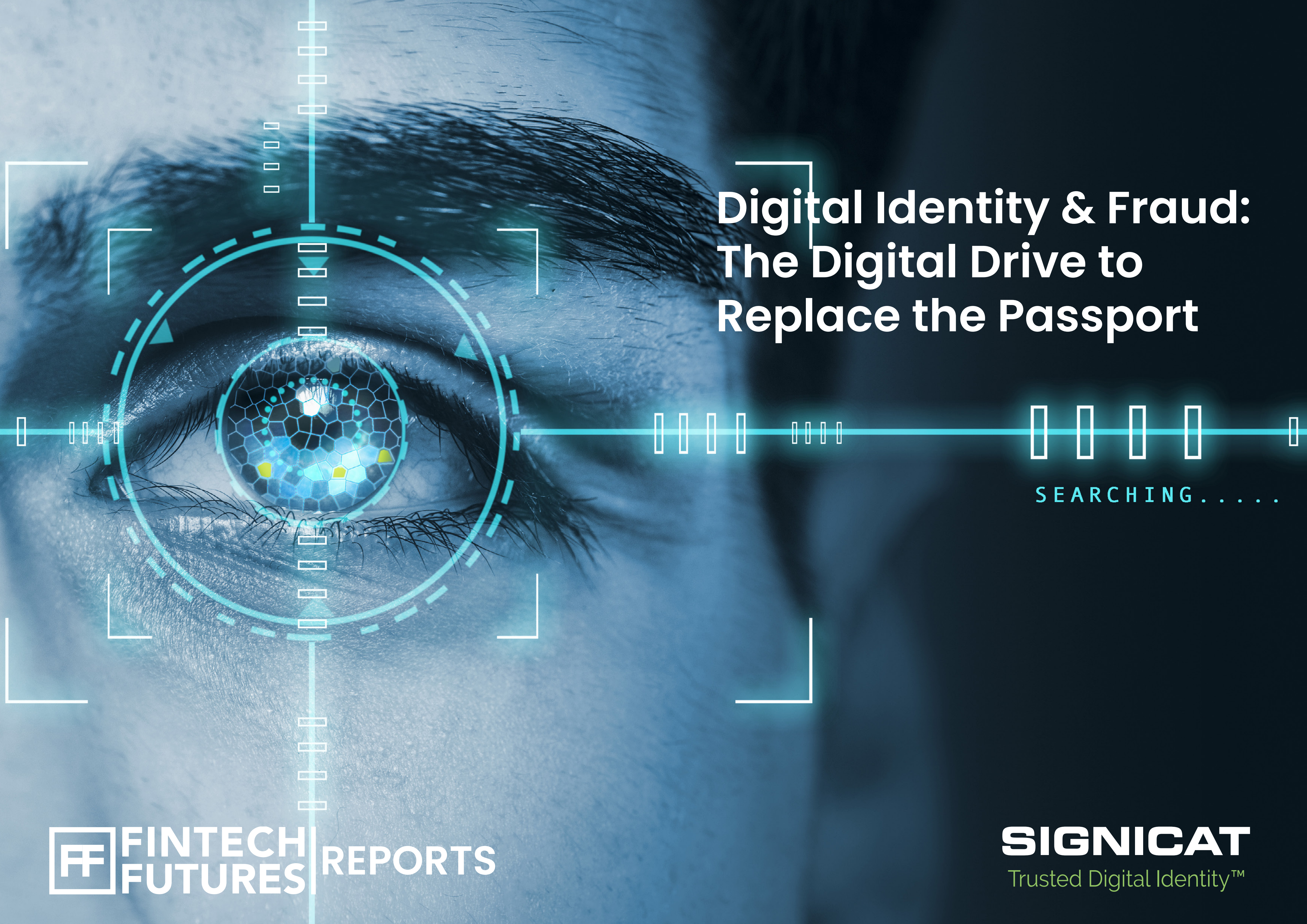
Digital Identity & Fraud: The Digital Drive to Replace the Passport



FF FINTECH FUTURES REPORTS

SIGNICAT
Trusted Digital Identity™

Introduction

Identification is a process which appears to have been left in the dust by technological advancement. While many digital options are available to customers when it comes to opening a bank account, taking out a loan, or creating an investment portfolio, the authentication stages of these processes still pull us back to an age where the paper document is king.

For most actions which require authentication the fallback remains a digitised version of an existing physical identification (the scan or photograph of a passport or driver's licence). When you consider that proper identification and know your customer (KYC) controls sit at the very heart of a vast majority of the financial services industry, it's not hard to imagine the role a digital replacement could play.

Information accuracy is critical for banks, brokers, intermediaries and lenders. The smudge on a poorly scanned passport image affects not only a firm's ability to offer prospective customers the right services but may also complicate its risk profile.

Regulators stand ready to lay massive fines at the door of noncompliant companies and are becoming increasingly interesting in gaining oversight on transactions. This makes a watertight and proper handling of data another persuasive argument for widespread digital identity.

Sitting outside of the interaction between regulator and compliance officer are the customers. As their worlds become increasingly digitised and real-time, they have begun to expect seamless experience in nearly every interaction in their lives. For many it just won't do for an account opening process to be held back by a week-long authentication process.

> “ Knowing your customer is a core capability of the banks. If a bank excels in this field, then this capability can be offered as a service or solution to their customers as well.
>
> As privacy and convenience take precedence, consumers are demanding 'new' digital identity services. Everything from access to football matches, identifying your plumber, getting access to a work site etc. is now digital and needs an identity solution.

Nico Strauss, tribe lead,
B2B services Rabobank

What is Digital Identity?

At its basic level, a digital identity is the combined attributes and information available online which can be assigned to an individual. It acts in the same way as an ID card or passport does in the physical world.

A person's online persona goes beyond their name, photo and address. It can include social media profiles, friendship circles, political opinions, shopping, location history, and browsing habits.

Identity provisioning and authentication utilises a three-tier system. At one end of the equation are the users. These are people in the system who are given an ID so they can carry out actions. Those users are verified by identity providers (IdPs), which usually take on the dual role of storing the information as well. Once the users have been cleared by the IdPs, relying parties take over the next stage of the process and open up services to a verified customer.

The rub is what the IdPs use to verify the authenticity of the user.

The Problem with Replacing Paper

Photo identification has been the de jure method of authentication for decades. It's a simple process – if the person standing in front of you looks like their photo then it's probably them[1].

The internet complicates things. For one, the person is no longer stood in front of you. As the oft-quoted New Yorker cartoon from 1993 foretells: On the internet, nobody knows you're a dog. Anonymity was a pillar of the early internet and it remains extremely important to many who surf the web.

So, how can your bank know that you're you?

"On the internet, nobody knows you're a dog"

When banks begrudgingly embraced the Internet 20 years ago, they encountered many of the same problems facing retailers, hoteliers, hospitality firms and even government agencies.

In response these institutions resorted to creating their own siloed, proprietary ID systems and databases for authenticating customer access to accounts. Now a username and a password were the keys to tying people to their sensitive information.

[1] Redundancy protocols come into play if the person stood in front of you happens to look exactly like the photo, but you still don't believe them. That's where birth dates and addresses come in.

£1.2 billion was stolen by fraudsters in the UK in 2018

This led users to have to embark on the same process for every service they wanted to use, banking or not. Everyone reading this paper knows the frustration of having to create unique passwords, email combinations and secure answers across dozens of websites.

When required to log into a bevy of websites every day, is it any wonder people turned to reusing the same credentials or reverting to that highest of security sins: "password1"?

Fraudsters have taken advantage of both sides of the market. In the UK in 2018, £1.2 billion was stolen by fraudsters and scam artists, an increase of 16% from 2017[2]. An estimated 4.7 million adults in the UK have been victim to credit or debit fraud, while trust in technology solutions has suffered – more than half (56%) of UK adults disrupt technology which automatically logs them into financial accounts[3].

If this consumer friction has created an opportunity for fraudsters, then the data repositories have become goldmines for cybercriminals. Proprietary ID systems consist of a veritable vat of personal data with some authentication controls layered on top. A single point of failure is all an enterprising hacker needs to gain access to a deluge of valuable information.

Millions of Records
+
Poor Endpoint Security
=
Hackers' Dream

Between 2006 and 2019 there were 18 data breaches in which more than 20 million data records were accessed by malicious third parties. In 2008 Heartland Payment Systems lost track of 134 million accounts; eBay had to warn 145 million users in 2014 that their account information had been breached; Yahoo lost between one and three billion records in what it called a "state sponsored attack" in 2013. Equifax, one of the largest credit bureaus in the US, blamed an application vulnerability for the exposure of 150 million accounts.

[2] UK Finance figures: https://www.ukfinance.org.uk/system/files/Fraud%20The%20Facts%202019%20-%20FINAL%20ONLINE.pdf

[3] Compare the Market: https://www.comparethemarket.com/media-centre/news/the-climbing-cost-of-fraud-over-2-billion-stolen-from-credit-and-debit-cards-in-the-last-year/

Regulatory Concerns

The seriousness of the issues around siloed data repositories and the loss of personal data has led regulators to sit up and take notice. In the European Union two new pieces of legislation dove-tailed each other into shaking up how data is stored and processed across the bloc: 2018's General Data Protection Regulation (GDPR) and 2019's second Payment Services Directive (PSD2).

Under the technical standards of PSD2 sits secure customer authentication (SCA). The SCA mandate requires all payments made by users to be authenticated using two out of three major elements: a password or security question; a phone or hardware token; and a fingerprint of face ID.

To address those needs payment standards firm EMVCo released the second version of its 3D Secure protocol (3DS). Where 3DS usually necessitated a user being sent to a separate secure webpage to input their data, 3DS2 requires just over 100 new data points to be sent from merchant to issuer.

The implementation date for SCA under PSD2 was set as September 2019. Following conversations with the industry and market participants, a managed implementation schedule was put in place by the European Banking Authority (EBA)[4], giving companies in Europe an extra window of opportunity to comply by 31 December 2020.

[4] https://eba.europa.eu/eba-publishes-opinion-on-the-deadline-and-process-for-completing-the-migration-to-strong-customer-authentication-sca-for-e-commerce-card-based-payment

SIGNICAT

The Battle to On-Board III

Why has huge investment in digital transformation led to so little change?

www.signicat.com

> “ Some institutions really have struggled with [PSD2]. Some of the clients I’ve dealt with have been on extremes. Some were extremely proactive and ready to go as soon as the legislation was drafted. Others were asking us what PSD2 was after the implementation deadline.
>
> There is some tension in the legislation. With PSD2 one of its underlying aims is to open up competition to the market, and to offer access to banking. On the other hand, its other aim is to ensure security. That is something that institutions will struggle with, because they have to find a balance between opening up access but also continuing to ensure customer confidentiality and security.
>
> There has been a great deal of regulatory change. Something like SCA affects any function which takes payments online. Every merchant has different requirements, different customers and different processes. It takes time to create an industry consensus around what something like SCA should look like.

Mardi MacGregor, senior associate, Fox Williams

Technical Solutions for Identity Management

While a ubiquitous identity standard may be some years away, there are plenty of technologies emerging in the market which can be used to regulate access to individual data repositories or help in creating a secure connection between separate silos.

A major advance in identity authentication has occurred with the proliferation of biometrics. With the introduction of fingerprint scanning, facial images, vein capture, device usage and channel behaviour, two new categories of authorisation have emerged:

What You Have	What You Know	What You Are	What You Do
Username	Password	Fingerprint	Keystrokes
Documents	Secret Word	Facial Image	Device
Smart Token	PIN	Voice Data	Browsing

The implementation of biometrics is not a panacea. While a 2019 report shows that the global biometrics markets will grow at a compound annual growth rate of 16% by the end of 2025[5], hackers will look at this new methodology as a fresh target for exploitation.

In August 2019 the fingerprints of more than one million people, as well as facial recognition information, usernames and passwords, was discovered on a publicly available database[6]. Biostar 2, a platform used by security firm Suprema, was found to be mostly unencrypted. Researchers gained access to more than 27.8 million records.

If your data is compromised and a fraudster attempts to impersonate you, behavioural biometrics kicks in. The methodology is useful for detecting account takeovers or new account fraud. Everyone has their own unique way of moving around a digital world. Fraudsters struggle to replicate exactly what the customer their impersonating would do.

Criminals are more likely to re-type details like names and addresses – things most people would know off by heart – or copy and past huge lumps of data. Yet the process of tracking this kind of activity is extremely labour-intensive and requires scripts to be embedded on almost all websites a user interacts with. It also raises that once a website knows your online behaviour, it could be passed on to third parties like advertisers.

[5] Global Biometrics Report: https://www.prnewswire.com/news-releases/global-biometrics-market-size-is-expected-to-grow-usd-42-904-56-million-by-2025-at-a-cagr-of-16-30---valuates-reports-300965345.html

[6] https://www.theguardian.com/technology/2019/aug/14/major-breach-found-in-biometrics-system-used-by-banks-uk-police-and-defence-firms

The Issue of Control

You have a digital persona whether you like it or not. Commercial, governmental and financial enterprises are edging ever closer to trusting the version of you made up of 1s and 0s than they are of your own opinions.

The decisions you make online directly affect your data profile and the way you interact with the world. The same mechanics that apply to profiling users for political campaigns can be used by banks for loan applications. China's social credit score system ranks each citizen on professional and personal interactions, to the minute detail.

When these actions in the physical and digital worlds are assigned to a profile associated with your username, password, biometric data and behavioural analytics it isn't hard to see why some are nervous of the lofty goal of a holistic digital identity, whether financial or otherwise.

> "At the moment there are still people who are just not interested in having a monopolistic online presence, and they don't want certain information about themselves to be made online.
>
> There is a temptation for people like us that are interested in the technology to overshadow those who use online or digital banking for a multitude of other seasons. There are a lot of people who are very anti-Facebook right now because of data privacy issues. As long as those people exist, there has to be a solution that works for them as well.

Mardi MacGregor, Fox Williams

> "In a more distant future, the use of blockchain for digital identity can be very promising. This self-sovereign-identity (SSI) could put the user in charge of his or her own data. No middlemen are needed to verify your attributes constantly. At Rabobank, we're heavily investing in. There are still challenges to be solved of course, but nevertheless; we want to be in the space as it develops.

Nico Strauss, Rabobank

Conclusions

There is a reason why digital identity is a hot topic right now. If there was a silver bullet for security online then we'd all be using it. As it is, every new innovation has a list of disadvantages almost as long as its advantages.

The speed of new developments in the marketplace, as well as the overhanging threat of regulatory punishment, means that banks and financial services firms can no longer thing of identity as an afterthought, or even as a mid-term development.

> “ There is a need to make a culture change within the bank to think differently about how we can support our customers. Culture doesn't change in months.
>
> Our response was to cluster digital identity together with payments and our open banking API's since they're often part of the same customer journey. For example, if you want to rent a car or apply for an insurance, you're going to need to identify yourself, prove your creditworthiness and pay for the product.

Nico Strauss, Rabobank

Digital account opening, authentication and identity changes are happening on a monthly basis and failing to keep track of the latest developments could leave firms with confused customers or an irritable compliance officer wondering why the regulators are tapping at the window.

Yet the idea of an all-encompassing digital identity for every user interaction seems one that is still some ways off. Trust is the key word here, and there just isn't enough of that around.

> “ Maybe we will get to the point where we have one solution for everyone, but it's going to be very difficult. If you think about things from a merchant perspective too, they are not going to want to cut out a portion of their userbase by have in authentication methods that only work for some people.
>
> For every person that has blazed a trail and innovated fantastic new ways of doing things, there are hundreds more who struggle to keep up.
>
> Siloed databases filled to the brim with poorly encrypted customer information have got banks into trouble in the past. Improving those data controls, however, appears a good base from which the industry can build towards a digital identity standard. Regulators are still focusing on the improvement of individual practices to protect customers. From that improvement consensus can be built, and from there the sky is the limit.

Mardi MacGregor, Fox Williams

Do You Manage Your Customers Digital Identity Lifecycle?

By Asger Hattel, CEO of Signicat

Signicat has been in the digital identity business for over 13 years, and one of the most dramatic changes we've seen in that time relates to what we refer to as Digital Identity Lifecycle adoption.

Digital Identity Lifecycle is the full digital experience your customer receives, from onboarding all the way through to the ending of their agreement. It includes digital onboarding, identity verification and validation, returning authentication, and providing integrated mechanisms to secure consent and signed agreements from consumers, all within a streamlined interface.

- Digital Identity Lifecycle goes beyond traditional web UX, and extends it to include four additional elements:
- Meeting your business needs regarding revenue and customer acquisition.
- Satisfying regulatory compliance such as KYC and AML requirements.

Reducing risk and fraud.

Providing your customers with an experience that is safe, satisfying and that builds trust in your brand.

In regulated industries such as financial services and insurance services, we've seen a big shift towards onboarding and servicing customers digitally. However, many initiatives are stand-alone and done somewhat in isolation from other critical customer touch points, resulting in a disjointed customer experience.

Customer Satisfaction and Conversion

In organisations that take a holistic view of their customers overall digital identity lifecycle, we see a dramatic upturn in customer satisfaction, customer retention, and customer conversion. Rabobank, for instance, increased customer conversion rates by 90% and saw a 13% improvement in customer engagement scores when it adopted a more holistic digital identity lifecycle approach for its customers.

Regulatory Compliance

According to Encompass Corporation, a total of $7.7 billion in fines were levelled at financial services organisations that violated AML regulations—an average of around $145m per fine in 2019. Strong digital onboarding and recurring validation processes that ensure compliance are now very much a must-have.

Reduced costs

While many consider setting up an end-to-end full lifecycle approach to be costly, we've seen many organisations reduce their operating costs. Aegon saved €100k in its first year by switching to a fully digital process. In Finland, Fellow Finance saw a reduction of 35% in onboarding costs. Most impressively, Rabobank saved €1.3 million over two years.

Sustainability

A final benefit to a fully digital identity lifecycle program is the dramatic reduction in paper use. Aegon saved some significant costs—but also saved a lot of paper: 2400kg in the first year alone. Coupled with the fact that onboarding times dropped from an average of four days to 30 seconds is testament to its decision to focus on the customer's digital identity lifecycle.

Asger Hattel is CEO of Signicat and has over 20 years' experience in financial services, technology, and telecoms. Before joining Signicat, Asger was Group Executive Vice President and CEO of Nets Merchant Services. Here, Asger headed up the Business Unit and increased growth, professionalised the unit, and integrated a number of acquisitions. Prior to his time at Nets, Asger was Executive Vice President and Head of Nordic and Wholesale Business for TDC, a Danish telecommunications company.

Asger began his career at McKinsey and Company and holds a master's degree in economics from Aarhus University.

FINTECH FUTURES | REPORTS

About FinTech Futures

FinTech Futures is a digital publishing platform for the worldwide fintech community – from the industry veterans to those just entering the space, and everyone in-between!

We provide daily news, in-depth analysis and expert commentary across a comprehensive range of areas.

Our broad readership and solid reputation, combined with in-depth coverage across fintech on a worldwide scale, makes us the leading resource for technology buyers, sellers, developers, integrators and other specialists across the sector.

Our website attracts nearly one million monthly page views and our daily newsletter is delivered to over 42,000 key decision-makers in the financial services and technology sectors. The brand is active across the key B2B social media platforms, with over 40,000 followers on Twitter @FinTech_Futures and over 21,000 members in our LinkedIn groups.

FinTech Futures Website: www.fintechfutures.com

Twitter: @FinTech_Futures

LinkedIn: @fintechfutures

Written by:

Alex Hamilton is deputy editor at FinTech Futures. He has been reporting on the financial technology sector for more than five years across a variety of industry publications and has written extensively on digital transformation, cybersecurity, and enterprise technology. He holds a masters degree in ancient history from the University of Nottingham.

He can be contacted at: alex.hamilton@fintechfutures.com

Reports & Surveys

Sponsorship opportunities are available for our surveys and well-researched topic-specific reports.

Visit **fintechfutures.com/reports-calendar** for a full list of our reports in 2020

TO REACH NEW PROSPECTS TALK TO:

Jon Robson
Head of Sales
Email: jon.robson@fintechfutures.com
Tel: +44 (0)20 3377 3327

Sam Hutton
Business Development Executive
Email: sam.hutton@fintechfutures.com
Tel: +44 (0)20 7017 7017