eBOOK

okta

Unlocking competitive advantage for fintech firms

How smart identity approach solves five core challenges

Unlocking competitive advantage for fintech firms

How smart identity approach solves five core challenges

Press to skip to

C **Contents**

Scene-setting:

Agility rules in the new normal

Over the last decade, investors have staked more than $25 billion in UK fintech firms. They're seeking to capitalise on this exhilarating sector's impressive instinct to innovate and disrupt; an instinct that has turned the UK into a world-leading location for fintech innovation.

UK fintech firms are rightly regarded as technology first-movers, ready to embrace new ideas from peer-to-peer lending and AI to crypto-currency. It's 76,500 strong workforce is third only to the US and the China in terms of job creation, economic contribution and its ability to attract venture capital. Perhaps that's why this sector has proved so financially buoyant, weathering first Brexit then Covid-19 uncertainty with apparent ease.

Paths are merging in this highly competitive landscape

According to Market Screener, the whole global fintech market will grow at a CAGR of 6% and be worth an impressive $26.5 trillion by 2022 . However fintech firms won't solely be competing against each other for a bigger piece of this attractive pie.

Traditional financial services megaliths themselves are becoming increasingly agile and customer centric, innovating in-house with rapid software development lifecycles. Telecoms companies are also entering the fintech innovation arena. PWC in its Global Fintech Report 2019 noted that the lines between sectors are becoming blurred as all seek to carve out new commercial possibilities. "Digital-only banks are offering redesigned client propositions and cost profiles. Investment managers are deploying fully customised robo-advice. Insurers are using sensors to monitor people's health and help prevent illness."

So which firms will best drive innovation and emerge as leaders, building truly open, agile and scalable businesses, fit for the new normal created by Covid-19?

The truth is that agility is nothing without security. Fintech companies increasingly hold highly sensitive, regulated customer data and IP that must be protected at any cost. Fintech leaders and solution developers need to adopt the right security approaches that mirror how solutions are used in today's accelerated, mobile, cloud-driven world — and do it for the lowest possible cost. That makes a smart approach to identity and access management (IAM) an absolutely key focus for success.

[1] https://www.mobindustry.net/7-key-challenges-fintech-startup-faces-and-their-solutions/

[2] https://www.pwc.com/gx/en/industries/financial-services/fintech-survey.html

Challenge One:

Starting up and handling rapid growth

Rapid growth isn't always a welcome problem, with companies often finding themselves having to on-board new staff faster than IT can handle. This is a particular problem in the fast-moving Fintech sector in which companies do often scale up to hundreds and even thousands of employees at unusual speed. Manual on-boarding processes tend to be expensive, clunky and disappointing for today's tech savvy workforce which expects work tools to seamlessly connect from the get-go, leading to a poor user experience and increased talent retention problems. Off-boarding leavers is another serious management headache. With many high impact breaches occurring when access privileges are compromised, how can firms reduce risk of exposure by quickly ensuring that they are promptly revoked?

To try and keep pace, the Financial Services sector has started rapidly adopting digital on- and off-boarding, and Fintech is now following suit. Processes need to be seamlessly unified and meticulously planned: consistent at all stages with the company's own brand. They also need to meet changing personal data security and HR regulations in the way that only a centralised and automated IAM service really can, helping companies to better manage their people right across the employment lifecycle.

Here are a just three advantages that the right Identity-as-as-Service (IDaaS) approach can deliver:

Manage user lifecycles remotely

In these times of pandemic, remote working is becoming the norm and many organisations are choosing agile, premise-light new operating models. Automating digital on- and off-boarding takes processes up into the cloud so employees can commence, manage and even end their journey online, without ever physically entering the office.

Enable secure, role-based access permission.

By pre-setting complex business rules and automating how they're applied through a managed IAM solution, employees can be accurately assigned permissions at role level, with the touch of a button. This significantly reduces the risk of employees accessing apps or resources they shouldn't. Fast, simple and compliant.

Prevent access and privilege creep.

It's common for access rights to start expanding as an employee's role morphs or they are assigned to work on different jobs. The intention is to enable productivity; the unintended consequence can be the granting of unauthorised access to sensitive information, leading to compliance issues and increasing the threat of a security breach. Having an automated IT policy that guides access stops this happening.

Challenge Two:

Smart end-to-end device management

Fintech sits at the heart of enterprise innovation, so people working in this sector will naturally want to work not just when and where but how they want, on any device they choose. That means device proliferation is inevitable in the average fintech working environment. Allowing open device access can enhance collaboration, drive productivity and improve the user experience and talent retention. Beyond that, many users will also want to bring their own applications to work. Managing the sheer number and type of devices within an organisation and open application access to ensure security can be a huge headache and resource drain. It can also slow innovation cycles down.

A best-in-class, centralised and automated 'one-touch' managed IAM service with open application programming interfaces (APIs) frees fintech firms to seamlessly and securely integrate their Identity Cloud with their chosen enterprise management solution, That frees the firm to manage their whole device universe with flexibility, ease and built-in compliance, enabling smooth and seamless device enrolment and administration access and establishing rapid device trust for managed devices.

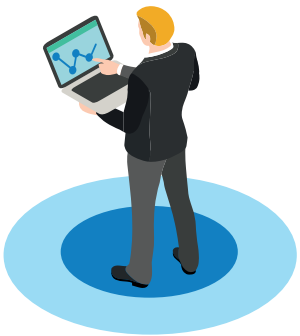
The result is that your talent can work on whichever the devices and apps they prefer, leading to a more engaged and productive workforce and less talent churn.

Empower Single Sign-On (SSO) and Multi-Factor Authentication (MFA)

Completely integrating with a core enterprise management solution enables seamless and secure authentication to all devices and company assets.

Deploy smart Device Trust solutions for Android and iOS

These allow IT admin teams to prevent unmanaged devices from accessing enterprise services through browsers and native applications. The latest innovations in production allow organisations to set and grant access to applications based on different device context such as managed via a device management solution; a known device that is un-managed and even restrict access to applications from unknown and unmanaged devices.



Easy user and group synchronization

For organisations running VMware WorkspaceOne, the enterprise management system can also access users and groups stored in the IAM services, eliminating the need to connect to Active Directory and simplifying the assigning of customized content and policies to devices that belong to users who are members of pre-set groups.

Challenge Three:

Optimising employee and partner productivity

Work now happens anywhere, on any device. For many, home-working is less a perk than a way of life. Mixed in-house and out-sourced teams need to collaborate and drive projects from wherever they happen to be. After all, the fintech sector is driven by innovation, disruption and collaborative brain-power. This kind of fast-moving, high-stakes environment demands high performing employees and extended partnership networks, supported by an effortless balance of collaboration, mobility and security. This frees everyone to focus on their roles, speed innovation cycles and drive competitive advantage.

In this 'API economy' how do fintech companies make their data and systems accessible from anywhere with identities and permissions seamlessly taken care of and APIs secured – so projects can keep moving while data stays secure and compliant? The answer lies in an approach that balances identity and device risks with the sensitivity of the service being accessed to create appropriate and differentiated security controls.

The wrong security measures can hamper the very productivity organisations are trying to enable. The smartest new cloud-based IAM services are built from the ground up to keep pace with digital transformation and support productivity with security features designed for enterprises where boundaries are blurred. The result? Fintech firms maintain high 'zero trust' security measures, while removing barriers that stop productivity in its tracks.

- Enable a frictionless work experience with SSO: Credentials that free them to only sign in once to all the systems, data, applications and domains they need. This reduces downtime and frustration for employees and cuts everyday help-desk workloads for IT. Key admin tasks such as password resets are also centralised.
- Create an extra layer of security with MFA: By requiring at least two pieces of evidence to prove identity, firms can make sure that users really are who they say they are. This frees users to access the best-of-breed apps they need through any device, without compromising data or increasing security risks.
- Stay flexible but alert: IT teams have the power to increase authorisation requirements – for example requiring an Adaptive MFA approach where behaviour demands it. That could be log in from an unexpected overseas location or new device or where the resource being accessed is especially sensitive, such as a finance system.
- Provide secure and efficient access for partners: Give partner networks open online access to key applications and systems such as CRM data, order booking and sales enablement tools, making B2B collaboration easier and more secure than ever.

Funding Circle

Empowering secure connections

The Funding Circle is a peer-to-peer lending marketplace that allows the public to lend money directly to small and medium-sized businesses. It knew that to successfully pursue its cloud-first strategy it needed a reliable and scalable identity solution across its user ecosystem. It chose Okta to supply SSO, Universal Directory, Adaptive MFA and Lifecycle Management for the 750 users operating its global lending platform — a foundation that then enabled it to rapidly deploy Slack for the entire global team. Employees, investors and businesses are now empowered to collaborate around the world, with consistent identity, reliable security and effortless access.

Challenge Four:

Ensuring cloud security without obstructing access

Cloud is scalable, agile and designed for companies with an innovative mindset. It also supports anytime, anywhere, any device access: ideal in a mobile, app-driven world. In fact, cloud can power the rapid, continuous development of new application-based services to meet changing market demand.

That's a big deal because applications are the innovation and productivity engine for fintech, with the cloud helping to accelerate their development, contain their cost and democratise their consumption. So to remain relevant and thrive in today's competitive market, fintech organisations need to keep harnessing the power of cloud computing in new and exciting ways, alongside innovative mobility approaches and customer engagement models.

No wonder then that fintech firms are not just early adopters of cloud — many are cloud-native, using cloud as a disruptive force on the path to wider and deeper digital transformation. 22% of all applications in the fintech sector already run on the cloud; a number that is only set to increase thanks to the obvious speed, cost and convenience advantages it delivers.

But how can firms counter the new security threats introduced by the explosion in cloud use?

Many fintech firms store, manage and process vast quantities of sensitive financial and personal data, that is highly sought-after by cybercrime groups and even nation states. Verizon claims that 80% of hacking-related breaches use stolen or weak passwords[3] which makes user account credentials the simplest way for malicious third parties to steal data. Employees pose even more of a security risk, with human error and malicious intent risking damaging data loss or theft. Honest mistakes made by staff regularly account for almost two-thirds of all breach incidents reported to UK watchdog the Information Commissioner's Office (ICO)[4].

Cloud-based Identity-as-a-Service (IDaas) is the only smart choice for securing the success of agile fintech organisations in a sector is also extremely highly regulated, by necessity.

- **Offering scalability and reliability that on-premise alternatives can't:**
  As well as a 360-degree view of all apps, users and devices in your environment.
- **Replacing outdated 'security at the perimeter' model:**
  This smarter approach secures access at the user level.
- **Removing the need to take cloud services offline:**
  By ensuring that new apps can easily be added and managed.
- **Offering integration to popular clouds such as AWS, GCP and Azure:**
  Federating with AWS SSO to enable single-click access to the AWS SSO user portal. This lets users access all of their AWS accounts in one place, automatically provisioning users and groups into AWS SSO and enabling centralised access to all of a firm's AWS accounts and resources.

[3] https://enterprise.verizon.com/resources/reports/dbir/

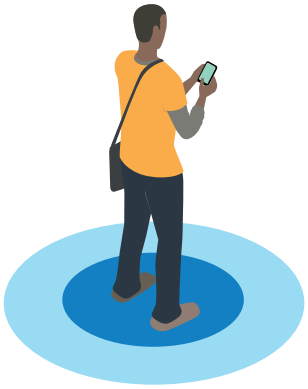
[4] https://www.infosecurity-magazine.com/news/human-error-to-blame-as-uk-data/

Challenge Five:

Creating a frictionless customer experience

Fintech solutions often rely on complex partner eco-systems to deliver the seamless products and services customer expect. Open APIs enable easy partnerships and securely bridge financial institutions, businesses and consumers: most notably useful in the digital payments sector. These APIs enable different software programmes and applications to communicate and interact with each other, driving exciting and innovative application models and a stand-out customer experience.

A smart IAM system with open APIs can help fintech firms build secure, seamless experiences for customers and deliver an approach to identity that developers and customers will love. By opening their APIs, fintech firms can access particular business or customer data and functionalities which they can seamlessly plug into their own applications to enhance what they can do.



By off-loading identity challenges to the right cloud-based IAM service and embedding identity into apps in a range of languages, fintech firms can create applications that:

Lower TCO by three times[5]

Compared to traditional identity management approaches

Transform customer engagement

Attracting customers and maximizing their lifetime value by creating advanced, frictionless, omni-channel and personalised digital experiences

Cultivate user trust:

By securing the customer identity lifecycle for apps and protecting them at registration, authentication and during in-app activity.

It no longer makes sense to devote expensive development team time to creating, managing and maintaining a bespoke IA platform when a great all-round solution can simply be deployed out of the box — and resource refocused back on the core business.

[5] https://www.okta.com/uk/customer-identity/

Next steps:

How an 'Identity Cloud' unlocks the future for fintech

The new decade brings with it new approaches to identity management as well as new security challenges. Cybercriminals never stop looking for new ways to steal data. For example new 'Deepfake' technology is now being increasingly weaponized for online fraud, with video footage or photographs superimposed on to source face or head and body using advanced neural network powered AI. It's all raising the bar even higher for online identity verification and security in an already ultra-competitive marketplace in which aggressive time-to-market is everything.

With competition for customers fierce and fintech firms seeking to deliver constantly-refreshed product portfolios with accelerated innovation rollouts, business models are constantly shifting to be more relevant, user-friendly and customer-centric. IAM is emerging as a vital tool in the arsenal.

Do-it-yourself approaches are time-consuming to create and easy to get wrong, which is why many leading fintechs are instead outsourcing IAM to a trusted strategic provider. The right identity cloud centrally takes care of securing access for employees, third party contractors, external business partners, administrators and consumers: all solved, on one integrated platform.

Partnership holds the key

Right now, Okta is working with fintech firms to create outstanding applications and services that will increase customer share and profit margins. Over 7,950 organisations, including innovative and agile names such as Paysafe, Funding Circle and Starling Bank alongside global brands like Adobe and Oxfam have built their digital transformation strategy around Okta identity and access management.

According to IDG, over half of firms (57%) have already deployed IDaaS for SSO and employee portals, while a third are using it to support MFA6 We believe that Okta cloud-based identity, also known as Identity-as-a-Service (IDaas), is the only smart choice for an agile fintech organisation.

- **Quick to set-up and easy to deploy:** Offering scalability and reliability that on-premises alternatives simply can't.
- **Securing access at the user level rather than at the perimeter:** Giving fintech firms a 360-degree view of all apps, users and devices in their environment.
- **Enhancing agility and easing compliance:** With complex financial regulations across diverse regions.

Like to know more? Let's talk

www.okta.com/uk

"The shifting of enterprise solutions to the cloud has created a complex architecture that requires more advanced IAM solutions than the ones currently offered by traditional identity management vendors."

Swapnadeep Nayak, Senior Industry Analyst, Frost & Sullivan.[6]

[6] https://ww2.frost.com/news/press-releases/proliferation-mobile-devices-and-social-media-drives-need-identify-and-access-management-iam-solutions/#respond