REPRINT

R&C risk & compliance

DIGITAL IDENTITY IN THE FINANCIAL SERVICES INDUSTRY

REPRINTED FROM:

RISK & COMPLIANCE MAGAZINE

JAN-MAR 2018 ISSUE

www.riskandcompliancemagazine.com

Visit the website to request a free copy of the full e-magazine

FORGEROCK®

Published by Financier Worldwide Ltd
riskandcompliance@financierworldwide.com

MINI-ROUNDTABLE

DIGITAL IDENTITY IN THE FINANCIAL SERVICES INDUSTRY

PANEL EXPERTS

David Pérez Lázaro
Managing Director
Accenture Security
T: +34 91 596 6000
E: david.perez.lazaro@accenture.com

David Perez Lazaro is the managing director responsible for Accenture Security business in financial services for Europe and Latin America and is based in Madrid, Spain. He has more than 20 years of experience in IT and information security and assists many Accenture financial services clients with the implementation of security from a business, technology and process point of view.

David G.W. Birch
Advisor
Dgwbirch Limited
T: +44 (0)7850 863 168

David G.W Birch is an author, advisor and commentator on digital financial services. He is global ambassador for Consult Hyperion, technology fellow at the Centre for the Study of Financial Innovation and a visiting professor at the University of Surrey Business School. He is an internationally-recognised thought leader in digital identity and digital money.

Matthew Thompson
Director, Business Development
Capital One

Matthew Thompson is an industry-recognised thought leader in the area of identity and security management and currently leads Capital One's initiative to bring innovative digital identity products to market as a service for businesses and consumers. He is an innovator in the digital identity space, having co-founded ID.me, which was named to the "100 Brilliant Companies" list in 2014 by Entrepreneur Magazine. Mr Thompson has spent years working in the public and private sectors to promote secure, user-friendly ways to give individuals and organisations confidence in their online interactions, which garnered him recognition by One World Identity as one of the "Top 100 Leaders in Identity" in 2017.

Nick Caley
Vice President, Financial Services and Regulatory
ForgeRock
T: +44 (0)797 919 9549
E: nick.caley@forgerock.com

Nick Caley is vice president, financial services and regulatory, with a clear focus on guiding organisations to deliver successful outcomes beyond compliance with GDPR, PSD2 and Open Banking. With over 20 years' experience covering all aspects of information security, Mr Caley has advised global clients in industry and government on security strategy and the operational capabilities that enable organisations to protect their most valuable assets.

R&C: Why has digital identity technology become a critical solution for the financial services industry?

Caley: Creating engaging customer experiences has become a critical success factor in determining the winners and losers in the rapidly evolving financial services industry. New market entrants and startups, across many different sectors, have disrupted established players and have stolen their market share due to a laser focus on user experience, convenience and better value. Digital identity is a fundamental element of creating a seamless customer journey across lines of business and different types of channels, be it web, mobile, contact centre or a growing ecosystem of partnerships. Given the regulatory demands of Know Your Customer (KYC), anti-money laundering, Open Banking, PSD2 and the EU General Data Protection Regulation (GDPR), digital identity helps financial services organisations not only achieve compliance but also develop innovative new products and services to stay competitive.

Thompson: Customers are increasingly expecting their financial institutions to deliver value whenever and wherever they are, and in that sense digital identity is both an enabling technology and cyber risk for the industry. The move to the cloud and mobile or connected devices has greatly expanded the number of applications that all financial services offer to their customers and digital identity is central to creating trusted interactions across those devices and applications. Further, digital identity technology can help by automating enrolment and providing security to enrolled customers in a scalable manner. Yet, increasingly sophisticated attacks require solid knowledge of who the customer is and requires multiple levels of control over how they access services.

> **"Creating engaging customer experiences has become a critical success factor in determining the winners and losers in the rapidly evolving financial services industry."**
>
> *Nick Caley, ForgeRock*

Lázaro: We are living in a new Big Data world, where data are more valuable when they are correlated. How? Identity is that enabler, a 'primary

key' for correlating interactions by individuals and devices through multiple channels, over time, from different locations, with different company brands or business units. In addition, a complete identity and access management (IAM) architecture that is easy to deploy, open and scalable is a must-have in the banking ecosystem, considering new regulations, business units and customer demands. There is no choice: KYC is the only way to survive in the digital banking world of tomorrow, and not being ready today could be a dramatic failure.

Birch: Online identification, authentication and authorisation are fundamental to the future of the industry because online everything is the future of the industry. Right now, the patchwork of identification and authentication solutions, the widespread use of identification as a proxy for what should be standardised credentials and the complexity of managing legacy infrastructure in new environments, means that the industry as a whole is being held back.

R&C: Could you provide an overview of how the financial services industry is using digital identity solutions? How are these systems helping firms to manage the challenges and opportunities of the digital age?

Thompson: Digital identity solutions are primarily used to verify a person's identity and then later authenticate that person to access permissioned services. Banks are able to monitor a customer during the session and if any action triggers an alert, that client will receive a 'step-up' authentication, such as "hold your phone up to your face and take a picture", which can then provide further assurances before allowing a higher risk transaction to occur. In effect, identity enables the bank to properly engage remote clients and manage risk for all transactions, whether it is a payment, a loan application or transferring money to another account. The combination of these activities, and frequent digital touchpoints, help increase the amount of trust between the party and their financial service provider. Mobile engagement provides organisations with a new dimension of trust that can be managed dynamically throughout the customer's lifecycle. This, in turn, allows friction to be applied to user transactions, based on dynamic risk, rather than a static set of rules that negatively impacts user experience and are easier for fraudsters to ascertain.

Birch: At the moment, most financial services organisations still use their own systems. But there are some interesting case studies – such as the Canadian multi-bank initiative — in more sophisticated shared and federated services. I would argue that they remain short of a fully-featured digital ID, but they are moving in that direction.

Lázaro: The financial services industry needs to deliver identity enabled services under a pressing demand to deliver more, faster, for less. This means a number of things. It means scale – identity platforms need to be elastic and capable of growing to internet scale. It means supporting identity services for millions of users. It means speed – clients need their identity platforms to rapidly stand up to environments that frequently use cloud solutions. Delivery methodology is shifting toward an agile and continuous delivery model to meet the connected timelines of front-end, user-interface teams. And it means sophistication – features such as advanced authentication have started to be integrated as standard within a short time frame, including multi-factor, risk-based or context-based authentication. Therefore, those companies that are able to provide the proper identity services with scale, speed and sophistication are ready to support digital age opportunities.

Caley: Financial institutions are using digital identity to unify fragmented customer identities that have been created across different lines of business, like retail banking and wealth management. Now, customers can have a single, consistent profile companywide, which enables contextual, personalised products and services. Delivered at scale to millions of customers, digital identity helps financial institutions to truly understand who their customers are and what they need, in order to deliver an omnichannel experience. Financial services providers are in a unique position as regulators demand they run KYC checks when accounts are opened. There is a demand to verify identity before being able to build trusted relationships with their customers. Beyond compliance, at the centre of digital transformation is an organisation's ability to recognise, identify, authenticate and protect their customers – wherever they are – at scale, in real-time and across a growing number of services, devices and connected objects.

R&C: How should financial services firms go about establishing a digital identity strategy? What are the key issues that need to be considered during this process, such as privacy by design and customer experience?

Lázaro: A next generation digital identity strategy should enable business by supporting secure adoption of new services, reduce administrative costs for managing users and their access by increased automation, reduce integration cost for new applications through centralised IAM capability based on repeatable processes, and reduce operational risk through streamlined and effective processes and ensuring people only have access they require to do their job. In addition, it should improve staff productivity by providing a single identity based on role and seamless user experience,

reduce security exposure by effectively managing external users and ensuring access is removed when no longer required, and improve compliance with security policy and regulations.

Caley: Financial institutions should consider five important elements to establish an effective strategy for digital identity. First, empower customer privacy. Keeping customer data secure is critical to protecting customer loyalty. It is also important to give those same customers granular controls over who can access their data, for how long and under what conditions. Second, secure the Internet of Things (IoT). Digital identity can connect and secure people, services and things within a digital ecosystem. This creates great opportunities for innovation around IoT-enabled financial services. The third element to consider is contextual security. It is imperative to provide continuous security verifying user authenticity and securing interactions to combat fraud and cyber attacks. It is a matter of measuring risk factors in real-time and requiring additional step-up security when needed. Fourth, companies should consider personalising the customer experience. By unifying on a single, customer identity profile, organisations can use contextual identity data to personalise the user experience. It also provides a single point where personal data can be managed, helping with data subject rights in GDPR. Finally, companies should implement identity enabled 'DevOps'. As the need for digital identity grows, it is important that the development team is supported with a suite of digital identity tools that integrate seamlessly into continuous delivery environments for agility and faster time to market.

> **"The financial services industry needs to deliver identity enabled services under a pressing demand to deliver more, faster, for less."**
>
> *David Pérez Lázaro, Accenture Security*

Birch: I tend to think that it is best to develop two related business cases: the cost-reduction business case and the revenue-catalysing business case. This allows for focus. I agree that it is hard to see how the revenue-catalysing services can be implemented in any other way than using privacy-enhancing technologies (PETs).

Thompson: Many organisations overemphasise the technical strategy of their identity solutions,

but often overlook the usability and customer experience impact. While the obvious building blocks of privacy and security should be the foundation of all effective identity strategies, the complexity of these solutions requires extra emphasis on the cognitive load they place on users.

R&C: What role does digital identity have to play with regard to ongoing developments such as open banking and payments-related legislation, such as the revised Payments Services Directive (PSD2)? To what extent can it assist with compliance obligations?

Birch: Both the cost-reduction business case and the revenue-catalysing business case come into play with regard to payments-related legislation. In terms of the cost-reduction business case, the banks have to implement something in order to comply, if nothing more. But if they are going to spend this money, then why not spend it in a more intelligent way and develop some positive, revenue-increasing opportunities as well?

Caley: At the core of Open Banking and PSD2 is user consent, which is tied directly to the identity of the customer and authorised parties. As we embark on the era of Open Banking for the first time, the customer owns their banking data and they choose who gets to access it and what they can do with it. Crucially, they can revoke that consent at any point in time. Financial service providers will have to ensure that sensitive data is secured and accessed in a controlled and consent driven way. The ecosystem of banks and third-party service providers, such as retailers or account aggregators, will have to become identity-enabled to take advantage in the benefits of this new world.

Lázaro: Digital identity is again a key aspect to comply with PSD2, as reducing fraud for end-clients is one of the key objectives and therefore stronger customer authentication is required, making two-factor authentication mandatory. Also, PSD2 requires the 'independency of channels', which means that the two factors must remain on independent devices. Using a full digital identity architecture, instead of point solutions for PSD2 requirements, will allow financial services organisations to comply with regulation with a long-term view in their digital transformation journey. The leaders who adopt this strategy will be better prepared for the future beyond short-term compliance requirements.

R&C: How can financial services firms use regulations like Know Your Customer (KYC), Open Banking and PSD2 as an opportunity for innovation?

Lázaro: Innovation in business processes and customer relationships in the new digital banking

world will be a key element to survive and beat competitors in the future. Those organisations that use regulation as an opportunity are on the right track: usually, regulation enforcement is driven by compliance without a business opportunity view. Now, it is time to face regulations as the vehicle to create a comprehensive digital trust environment to help the company to become a market leader. It is time to build the relationship between compliance, security and business units to create a different approach and the ambition to innovate – to use regulations as an opportunity instead of an obstacle.

Caley: Given the significant investments already made in KYC processes, financial services firms have a tremendous opportunity, through innovation and collaboration, to extend trusted identities and their attributes to new services and develop further revenue streams. Access to customer accounts via APIs enables the provision of entirely new types of service that are regulated under PSD2 – namely third-party payment initiation, provided by payment initiation service providers (PISPs), and third-party account access, provided by account information service providers (AISPs). We expect to see the provision of highly customer-centric, digital financial services portals that leverage customer insight gained through access to a more complete view of a customer's financial transactions. Such services can enhance customer loyalty, as well as open new revenue opportunities for both banks and third-party providers.

Birch: One obvious way to explore opportunities for innovation is to go out into the market and look at what the RegTech startups are doing, then either buy them or partner with them. I think that for many organisations, the business case around RegTech is actually better than the business case around FinTech, because the costs of KYC and

related compliance are so high. One of the reasons why banks have slashed their front offices, yet only seen modest cost reduction, is the rising cost of compliance.

R&C: As trusted custodians of personal financial data, how should financial services organisations be preparing for the impact of the EU General Data Protection Regulation (GDPR)?

Caley: It does not have to be all doom and gloom. Committing to the right approach can help financial institutions put transparency and control into the hands of the customer and ultimately build trusted relationships that differentiate an organisation from the competition. With identity, there is an opportunity to develop a mutually beneficial value exchange built on trust. In return for a richer user experience, customers will share more data if they can trust what will be done with that data. And as organisations are tasked with processing and storing this data, they need a comprehensive identity platform to be successful. This platform needs to provide a single view of the customer to give users a place to view and manage their profile data, no matter where it is stored; as well as a comprehensive set of end-user privacy capabilities for obtaining and proving consent, data minimisation and data accuracy and the ability to implement an erasure protocol.

Birch: It is impossible to overstate the impact of GDPR. For most companies it will turn personal data into toxic waste. I think regulated financial institutions should seize the opportunity to become the customer's friend here: "let us keep the customer data safe and sound under lock and key in the institutions and put our arm around them when they venture out in to the online world".

> **"It is impossible to overstate the impact of GDPR. For most companies it will turn personal data into toxic waste."**
>
> *David G.W. Birch, Dgwbirch Limited*

Lázaro: GDPR impacts all aspects of the banking operating model, from customer-facing product marketing, client on-boarding to back-end data processing, risk management, security and even HR and employee-related operations. This means

a huge transformation in the way personal data – and particularly customer data – are managed today. There is a long list of aspects that are getting attention, but I would highlight a number of questions that financial services should ask now to be compliant before 25 May 2018. Do we have a trained DPO? Can we erase a customer's data, or tell them what we hold? Do we have granular consent from all data subjects? How are we preventing data loss? Could we report a data breach within 72 hours? The answers to these questions are too complex to solve in a short period of time. Banks' challenges are probably less than other industries, as customer financial data are the key assets of the bank and security maturity is higher than in other industries, but it is true that the complexity of ensuring data mapping and the right access to customer data is also greater. The game has just started – and it will last beyond May 2018.

R&C: As customer financial data is increasingly shared with third parties via application programming interfaces (APIs), how can financial services institutions ensure that customer privacy and consent is respected?

Thompson: Aligned with the Consumer Financial Protection Bureau's recently released principles for protecting consumer-authorised financial data sharing, APIs can provide transparency and help consumers share their financial data with trusted third parties in a way that is within the consumer's control. It is in the best interest of consumers that third parties maintain transparency with their users about how data will be used and protected throughout the entire lifecycle of personal and financial data sharing. Parties should never have to share their credentials to obtain data.

Lázaro: APIs are used to connect to banking back-end systems and expose business data, functionality and services to the outside world in a controlled fashion. A robust API security architecture is mandatory to maintain high security for customer data, balancing openness and control. There are four key elements of API security architecture: identity, privacy, threat prevention and rate limiting and throttling. Privacy architecture should guarantee data are managed following industry or general regulations like GDPR that addresses specifically how the customer is the owner of his or her data and should have full control – including explicit consent – of data usage. This aspect puts identity in the middle, to ensure all the customer data are properly mapped and accessible, linking them to customer identity.

Caley: The primary challenge to solve is that of customer consent, a requirement of Open Banking, PSD2 and GDPR. Consent is critical for respecting consumer data privacy. Financial institutions that need to comply with Open Banking and PSD2 must

gain explicit customer consent for the execution of payments and for third-party access to data. For GDPR, it is important to ensure that data will not be used for any purpose other than that requested by the customer. Today, many financial institutions lack the required mechanisms for collecting granular consent, and both regulators and customers will expect more than pre-populated opt-in checkboxes. Leading organisations will design their services based on the User-Managed Access (UMA) standard, which is viewed by experts as the future of consent management for both Open Banking and PSD2. UMA empowers users to share data with each other, not just with third-party organisations and at any point revoke that consent as required by the GDPR.

Birch: Here is where new technology may well deliver some of its more important – and counterintuitive – results. The ability, for example, to use homomorphic encryption and zero-knowledge proofs to provide 'audible privacy' means a new generation of products and services. We should stop talking about trade-offs between security and privacy and commit to delivering both of them.

R&C: Cyber security threats continue to increase in volume and sophistication, and financial services firms are popular target for hackers due to the valuable data that they hold. How can digital identity help organisations to manage this risk and secure their operations?

Lázaro: Identity has its role in facilitating cyber security, both from employee and customer perspectives. There are several use cases, some of them related to well-publicised threats and breaches, where digital identity plays a key role to protect bank assets from abuse of privileged user accounts or unmonitored service accounts, from malicious use of accounts by internal employees, from hijacking of orphaned accounts from leavers and, last but not least, from proliferation of unnecessary access gained through past job history. On the other hand, customers are a weaker link than employees and the failure of the consumer to safeguard their own credentials can equally make the news. A poor standard of passwords or sharing credentials across other sites which are breached can still affect a firm's reputation. Under these circumstances, large financial services SOC/CERTs are integrating 'identity-based' monitoring and analytics information to proactively and reactively mitigate cyber threats.

Birch: In essence, I think that the way forward on cyber security is to keep customers' identities, credentials and reputations in the bank vault.

Caley: With a modern digital identity platform, financial institutions can protect against malicious

attacks and identity fraud through multi-layered security models. The more that people, services and things are accessing network data and applications, the more that security teams need to be on the ball when it comes to balancing security and accessibility for a seamless customer experience. Through contextual authorisation and adaptive risk features, organisations can verify the authenticity of users, devices and things continuously throughout a session and mitigate risk whenever an anomaly is detected. Continuous security evaluates the context of the request for additional identity verification when something unusual takes place, like a resource request from an unfamiliar location or device. Integrating identity context within the security response capability allows financial institutions to monitor users and their activity, with alerts for changes to identity and access behaviour in user activity reports.

Thompson: When it comes to digital identity, it is important to use a layered, risk-based security approach to remove any single point of failure. According to the 2017 Verizon Data Breach Investigations Report, 81 percent of data breaches were attributed to weak, reused or stolen passwords. Once a phishing email gets through to a single user on the network, they must move laterally across the network to find the data worth stealing and often, those data stores require higher access privileges. Malware enabled with keystroke logging routinely collects logins from admins which then escalates privileges for the hacker. If an enterprise is using multi-factor authentication with out-of-band communications to a mobile device or is running behavioural software tied to identity, those breaches would have been less likely to occur. We must know with certainty who is operating on the network, what permissions they have, and when they access those valuable data stores we need the ability to apply strong authentication measures to ensure it is them. The identity credential and behavioural analysis can then be combined with all other security technologies to provide defence in depth.

"According to the 2017 Verizon Data Breach Investigations Report, 81 percent of data breaches were attributed to weak, reused or stolen passwords."

Matthew Thompson, Capital One

R&C: Today's customer expects a personalised, omnichannel experience.

How can digital identity help financial services firms to build these trusted relationships with their customers?

Caley: Unifying customer identity is critical for creating a seamless, omnichannel customer experience. The information linked to customer identities helps financial service providers to accurately and to authentically interact with customers across all channels. With a complete understanding of customer preferences, providers can actively engage customers with personalised offers, timely alerts and other individualised experiences. Banks, insurers and FinTechs can reach their customers with personalised marketing campaigns that show that they know and understand their customer. By building customer-driven digital ecosystems, providers can exceed customer expectations with dynamic experiences that change to match shifting customer needs and preferences.

Birch: Customers rightly expect to be able to access financial services 'anywhere, anytime and any place'.

Thompson: Depending on the customer, you will have a different form of access to services. Certain customers may prefer showing up at a branch or accessing their accounts from a home computer, while others will prefer to access banking apps via their mobile device. Identity verification and authentication technologies can flow seamlessly between these channels and enable the bank to perform uninterrupted service as the customer goes about conducting their financial transactions. Apps and software now bridge all forms of access and the customer's identity enables analytics to better serve them based on their financial profile, as well as where they are likely to be contacting the bank from. This means the ability to reduce friction, while delivering faster services that are tailored to the customer's needs.

Lázaro: Identity is the cornerstone for digital banking to increase value in business-to-consumer, ensuring a comprehensive and holistic view of user journeys across systems and enabling a consistent, personalised, relevant service regardless of channels and technology platforms. This means that an identity and access management architecture is a pillar of any digital banking transformation journey, so those banks that embrace IAM solutions in this way will have a long-term competitive advantage to win the digital race. The digital trust concept starts with digital identity, ensuring that a customer's identity and his or her data are properly enabled and protected by the right IAM processes.

R&C: Looking ahead, what are your expectations for the continued evolution of digital identity in financial services?

Lázaro: A frictionless customer experience is at the top of any digital banking transformation, so IAM solutions will evolve to provide – or integrate third-party products than can provide – these frictionless capabilities, mainly through biometrics. The use of biometrics for identity management will become a new normal in the future and the financial services industry will be an early adopter out of the traditional use for border management or national ID programmes that have proven these solutions at scale. Another area of evolution is the rather slow convergence of business-to-employee and business-to-consumer identity management, considering that there is now a blurred line between how a consumer or employee interacts with applications, services and the IoT. Identity and contextual management is more important than ever to manage this convergence and consumerisation and, finally, it does not necessitate a single identity platform, but promotes a harmonisation of business process, infrastructure and delivery model. In the future, managing thousands of employees' identities will probably be just an 'extension' of millions of customers, as another outcome of the strong digital transformation of banking services.

Caley: The real opportunity offered by the use of a digital identity platform is for financial institutions to get to know, interact and connect more deeply with prospects and customers across any channel – be it cloud, social, mobile or the IoT. Organisations can use the management of consent to earn a far greater degree of customer trust by giving customers control over who gets access to their data and for how long. In this way, digital identity powers a far more effective digital transformation as organisations gain a better understanding of their customers when they share actionable information on preferences, habits and choices. This can be used to create authentic, engaging customer experiences that contribute to loyal customer relationships.

Birch: Right now, I can see three broad paths through the digital identity landscape. The 'identity problem' is not going to go away, so someone will have to fix it. This might be the government, it might be the banks or it might be someone else. If it is someone else, it will be the internet giants, and this may not be to the banks' advantage. Hence, I am hopeful that the banks will find ways to cooperate and move forward. They can share the cost reductions by sharing infrastructure in response to the current demands from open banking and then compete on services using that infrastructure, whether it is centralised, federated or even decentralised through technology such as blockchain. R&C