# DIGITAL TRUST WORLD 2021


## The Conference for Authentication, Biometrics, Fraud & Security and Identity

SPONSORS & PARTNERS

BehavioSec
ENTRUST
mobbeel
nok nok
Age Check Certification Scheme
cifas The UK's Fraud Prevention Community
digital trust networks
fido ALLIANCE simpler stronger authentication

MEDIA PARTNER

BIOMETRIC UPDATE.COM

GOODE INTELLIGENCE
YOUR PARTNER FOR BUSINESS RESEARCH & ANALYSIS

# AGENDA - Day 1



*All times shown are in British Summer Time (BST)*

**11:30-11:50 Welcome & Analyst View**
Alan Goode, CEO & Chief Analyst, Goode Intelligence.

**11:50-12:50 Digital Trust World Masterclass with Cifas**
Cifas, the UK's Fraud prevention community, shares the best ways to fight fraud in your organisation in this exclusive Masterclass. With special guest speakers, Nicole Gibbs and Neil Jordan.

**14:00-14:30 Identity Visionary 2021: An interview Emma Lindley**
Michelle Goode interviews Emma Lindley, Goode Intelligence's Identity Visionary 2021.

**15:00-16:00 Digital Trust World Masterclass: Rethinking Digital Identity**
Alan Goode chairs and moderates a panel of experts: Steven Grant, Kirsty Innes, Dan Johnson, Dr Manreet Nijjar, Andy Smith and Sandra Trenevska to discuss how identity verification plays an essential role both now and in the future.

**16:00 Close of Day 1**

# AGENDA - Day 2



*All times shown are in British Summer Time (BST)*

**10:30-10:50 Welcome & Analyst View**
Alan Goode, CEO & Chief Analyst, Goode Intelligence.

**10:50-11:50 LIVE Panel & Discussion: The biometrics journey to support a real digital identity**
Join this live discussion with José Luis Huertas to hear about the biometrics journey to support a real digital identity. Topics include the evolution of mobile biometrics, the importance of multi-biometrics and liveness detection, future evolution and how to secure the signature process with biometrics and identity verification.

**11:50-12:50 Digital Trust World Masterclass with ACCS**
What does ICO's approval of the UK GDPR Certification Scheme for Identity and Age Assurance mean for identity service providers and how can relying parties start to specify certification and assurance in procurement tenders? Find out how in this exclusive Masterclass with Tony Allen.

**13:30-14:00 Biometrics Visionary 2021: An interview Dr. Neil Costigan**
Alan Goode interviews Dr. Neil Costigan, Goode Intelligence's Biometrics Visionary 2021.

**15:00-16:00 LIVE Panel discussion - Behavioral Biometrics: A versatile technology for fraud detection and authentication**
Chris Ralis will share his insight on how BehavioSec is using Behavioral Biometrics to combat sophisticated digital fraud attacks while still delivering a seamless user experience. Followed by a panel discussion with Jordan Blake and Alan Goode, moderated by Chris Burt from Biometric Update.

**16:00 Close of Day 2**

# AGENDA - Day 3



*All times shown are in British Summer Time (BST)*

**10:30-10:50 Welcome & Analyst View**
Alan Goode, CEO & Chief Analyst, Goode Intelligence.

**10:50-11:50 Digital Trust World Authentication Masterclass with the FIDO Alliance**
A special FIDO Alliance Masterclass brought to you by Andrew Shikiar.

**13:30-14:00 Authentication Visionary 2021: An interview Phil Dunkelberger**
Alan Goode interviews Phil Dunkelberger, Goode Intelligence's Authentication Visionary 2021.

**14:00-15:00 LIVE Panel discussion: We have been promised a Passwordless future, so where is it?**
Passwords have been around since the 1960s and were originally designed for a small amount of users connected to mainframe computers. Fast forward to the early 2020s and billions of computer accounts still rely on them for authentication. They are insecure and inconvenient, but for many accounts they are still the primary method of authentication. This panel, sponsored by Entrust, examines why this is and takes a look at what Passwordless alternatives exist that comply with standards, are convenient and secure. With panellists Rajan Barara, Jenn Markey and moderated by Alan Goode.

**15:00-16:00 LIVE Panel discussion - Behavioral Biometrics: A versatile technology for fraud detection and authentication**
Chris Ralis will share his insight on how BehavioSec is using Behavioral Biometrics to combat sophisticated digital fraud attacks while still delivering a seamless user experience. Followed by a panel discussion with Jordan Blake and Alan Goode, moderated by Chris Burt from Biometric Update.

19:00-19:45 Future View with Nok Nok Labs
Alan Goode discusses Picturing Authentication in 3 Acts: The Legacy, The Possible and The Road Ahead with Rolf Lindemann

**16:00 Close**

# DIGITAL TRUST WORLD 2021

## WELCOME

### *The matter of trust in a digital world*

Welcome to **Digital Trust World 2021!** Trust is at the heart of fruitful relationships – both personal and professional – for both the physical and digital worlds. In the physical world, trust is created through security, effective process and reputation. In the digital world we need to match the levels of trust that thousands of years of human civilisation has created to maintain a safe and prosperous society. Digital transformation is accelerating at an incredible rate across the globe. How we recreate the trust of the physical world, and even improve on it, is one of the fundamental questions of our time.

I hope you enjoy the conversations and discussions over the coming days. All our sessions are being recorded and will be made available on demand shortly after the event to registered attendees so no matter where you are in the world, you can watch at a time that suits you, making this event especially convenient for our global audience.

Finally, special thanks to our sponsors, partners and speakers who have made this event possible.

Alan

# BIOMETRICS IN PAYMENTS: THE CHALLENGE OF COVID AND CUSTOMER CHOICE

Alan Goode,
Goode Intelligence

**Biometrics has transformed global payments and has quickly become the go-to technology to provide secure and convenient identity verification (proofing), customer authentication, transaction authorisation and support for fraud detection.**

To achieve this, a range of biometric technologies are being deployed across all payment channels, from the traditional to the emerging, and across a wide variety of payment scenarios. These include mobile wallets and payments, biometric payment cards, eCommerce solutions, drawing cash from ATMs or directly at physical retailers (tokenless or 'naked' payments), as well as pilots and proof-of-concepts (POCs) with wearable devices (wPayments), and even via IoT devices including connected cars.

Driving this adoption are the challenges that customers want choice for payments, and that their payment experience must be convenient, with as little friction as possible. Any delay in the process can lead to cart abandonment and that is not good for retailers, merchants and payment service providers alike. The average online cart abandonment rate currently stands at 70%, with 31% halted due to friction – often caused by frustration with the identity and authentication processes. Consumers want instead payment experiences that combine convenient identity verification, user authentication and payment fraud reduction. They also want the assurance that payments are secure and safe; and in the era of Covid-19, they want to be able to make them in an hygienic manner.

"Biometrics are a key part of a payment service provider's toolkit in the never-ending task of reducing financial fraud and ensuring customers can conveniently prove their identity"

## Biometrics a must-have

In these circumstances, biometrics for payments is becoming a must-have technology. A recent Goode analyst report [1] forecast that $5.765 trillion worth of biometric payments will be made annually by 2026 across the world. In effect, biometrics has become a key part of a payment service provider's toolkit in the never-

ending task of reducing financial fraud and ensuring that customers can conveniently prove their identity and authorise transactions when paying for trillions of dollars' worth of goods and services in a variety of payment channels. But there are a number of major ongoing challenges in this. They include:

**Meeting payment regulation and standards**

A mix of regulation and industry standards are now in place that present a number of key questions when using biometrics for payments purposes: how and where is each customer's biometric data being stored? Who has access to it? How well is it protected? When a person enrols their fingerprint on a smartphone, is it stored in secure hardware and does it ever leave the security enclave? What legislation and regulations are in place to cover the privacy and security aspects of biometric technology? It is clear that biometric technology can match, and possibly exceed, all the above requirements. It meets the EU's PSD2 Strong Customer Authentication (SCA) technology standards requirements as part of a multifactor authentication approach that includes 'inherence' (biometrics) as one of these factors. It is also supported by the EMVCo's latest 3D-Secure technology standards to improve security in card-not-present (CNP) scenarios.

**The impact of Covid-19 on payments**

The Covid pandemic has accelerated a number of key trends from the last 20 years, which can be collectively classified as 'digital transformation'. We're moving away from physical to digital service delivery, performed on any device that can run an app or load a browser. This affects most industry sectors, but is especially acute in retail and financial services where physical stores and bank branches are being replaced by remote digital services.

In addition to the impact of social distancing on the physical world, activities like touching sensors on shared devices have been restricted during the pandemic. For payments, this includes sensors integrated into shared devices such as ATMs, point-of-sale (POS) systems and kiosks. This is accelerating the decline in the use of cash globally.

After an initial spike in cash withdrawals ahead of lockdowns around the world, the use of cash has been dented by concerns over transmitting Covid-19 via high-traffic ATMs. According to figures from Worldpay [2], cash use at the POS fell 32 percent from 2019 to 2020. Worldpay estimates that Covid-19 has accelerated the decline in cash by three years, with cash being used for 20.5 percent of global POS transactions in 2020, down from 32.1 percent in 2019.

All this is making biometric payment cards even more attractive, with consumer demand for these cards increasing during the pandemic. A 2020 survey carried out by Goode Intelligence in partnership with G+D, Linxens and NXP, found that 88 percent of UK consumers wanted their bank to upgrade their contactless payment cards to support biometrics. In addition, 42 percent of respondents were willing to pay between £2 and £5 a month for a biometric payment card with no upper spend limit.

In the longer term, the requirement for hygiene in physical payments means that organisations may look to

deploy ‘contactless’ biometric sensors in shared and public spaces. We have already seen technology integrated into airports that allow passengers to ‘wave’ their hands through a reader. This does not necessarily mean that organisations will avoid fingerprinting as a modality – just that it will be touchless.

This will not affect biometric sensors used in devices that are not regularly shared and where a single user will enrol and verify – such as in smartphones or biometric payment cards. Contactless card payments were already growing before the current crisis, and figures from Barclaycard UK and Mastercard show that this growth is accelerating. Mastercard is reporting a 40 percent rise in the use of contactless payments/cards worldwide. The increase in spending limits on contactless is probably also helping this upward trend.

There is also now a demand for hybrid devices that can both identify people, and perform a quick ‘at range’ biomedical check on them to determine if they may have been infected. In China, these devices have not only been deployed at borders and transport hubs but in bars, cafés and retail stores. Longer term, this could potentially kick-start the use of combined biomedical and biometric systems in wearables – such as smart watches, wrist bands and clothing – to create applications that know who you are and how you are. These systems would be able to check body temperature, blood pressure, ECG and heart rate while also knowing the identity of the person (patient).

However, there needs to be an adequate privacy and trust framework to support this collection of sensitive personal data – and it remains to be seen if these ‘emergency’

measures will become permanent once we are out of crisis mode. It is important for businesses to assess the risk of the current crisis, and to ascertain what the 'new normal' is and how long that new normal will be with us. It is important to recognise that some of the measures now being deployed will stay with us once we return to normality.

**The rise of mobile wallets powered by biometrics**

Mobile wallet use, often authenticated by on-device biometrics, has accelerated in the last two years, making it a favourite payment mechanism alongside contactless payment cards. Covid-19 has played a part in accelerating this trend, especially the use of mobile wallets at the point-of-sale – where they provide a 'safer' method of payment than cash and also PIN-authenticated debit and credit cards.

Worldpay, in its latest annual payments survey, reports that mobile wallets have gained on the back of the decline in cash, with their use rising 19.5 percent between 2019 and 2020 to now represent 25.7 percent of all point-of-sale transactions [3]. Worldpay also forecasts that by 2024, mobile wallets will account for 33.4 percent of global POS spend, with their adoption in the APAC region being higher at almost 48 percent of spend.

Analysing this trend, Celine Savaton, IDEMIA's marketing manager for financial institution digital solutions, believes the lines between channels and the technology used in them is 'getting blurry'. Savaton explained: "As a smartphone wallet can be used for both in-store and online, what is crucial to the use of biometrics to support payments is the cross-channel experience." Usage is also "getting blurry" in terms of the definition of what a payment is and looks like: transactions supporting ticketing, identity and travel are being 'hybridised', and service providers and platforms are realising the opportunity that this offers. A single verified identity credential can be linked to permission to travel, to hire a vehicle, to enter a sports stadium and to pay for goods and services.

Overall, there is a great deal of innovation occurring with biometric payments, especially in the area of tokenless payments. Goode Intelligence believes that for physical payments, and hybrid payments where other applications including identity and ticketing are combined, tokenless transactions will eventually prevail.

**Increased adoption of biometric payment cards**

There are a number of favourable conditions helping to accelerate the adoption of biometric payment cards. Demand from consumers is strong, card prices are dropping for issuers, and card scheme certifications are increasing. The number of pilot schemes has risen significantly, commercial rollouts have begun, contactless card adoption has increased, and the ecosystem is creating valuable partnerships. As a result, Goode Intelligence forecasts that by 2026, at least one fifth of all payment cards shipped will be biometric.

Biometric payment cards operate in the same way as normal cards, except that users have to authenticate themselves using their enrolled fingerprint, thus replacing the PIN. If the fingerprint presented successfully matches the template stored on the card, then an EMV authenticated and authorised transaction will go through on the point-of-sale

terminal, below or above the transaction limit. If the match is unsuccessful, then the card cannot be used without falling back to its original PIN. This means that the card is useless without the presence of the legitimate owner; and if the card is lost or stolen, it cannot then be used in contactless mode, as is the case with standard contactless payment cards.

The Goode Intelligence, G+D, Linxens and NXP survey mentioned above reported a number of findings in relation to consumer demand for biometric payment cards, including:

- 95 percent of respondents prefer using a contactless payment card for in-store transactions
- 76 percent of respondents are now significantly less willing to use a shared PIN-Pad as a result of Covid-19
- 85 percent of respondents now use contactless payment cards more as a result of Covid-19
- 42 percent of respondents are willing to pay between £2 and £5 per month for a biometric payment card with no upper spend limit
- 88 percent of respondents want their banks to upgrade their contactless payment cards to support biometrics

**Automotive biometric payments – the pay anywhere, any time revolution**

Automotive, in-car payments offer a means for vehicle drivers and passengers to pay for a range of goods and services, typically without getting out of their car – such as road tolls, petrol, electric charging, car rental, ride-sharing, or drive-through food and drinks. Much of the infrastructure needed to support such automotive payments exists within payment card scheme tokenisation technology. This also has the potential for use beyond the automotive market – such as payments for IoT smart home devices, including smart speakers and smart TVs. Whether you use a token or the device itself (nominally a smart mobile device) is a deployment choice.

"The new Mercedes-Benz S-Class car will feature fingerprint sensors built into the dashboard, face recognition supported by two cameras, and the capability to use voice biometrics"

In line with this, Mercedes-Benz announced in July 2020 that its new S-Class car will come with biometric technology integrated into its infotainment system, enabling “verification of digital payment processes from the vehicle”. The car will feature fingerprint sensors built into the dashboard display, face recognition supported by two cameras, and the capability to use voice biometrics. The infotainment system is called ‘My MBUX’ and supports four different methods of authentication, three of them biometric.

It is becoming clear that the future of payments may well be tokenless: no card, no phone, no watch – just you. The ever-improving performance of biometric systems means these systems could become good enough to be used on their own without a token to authenticate customers and approve payment transactions – the ‘pay by me’ service.

When this will become dominant and replace token-based payments is difficult to estimate. But Goode Intelligence forecasts

that by 2026, 302 million people globally will be using tokenless payment solutions. The arrival of Amazon Go and the use of Amazon One also offers an insight into the future of physical retail stores, which could be replicated in areas like mass transit travel (ticketing), events, car rental and car ridesharing and sports stadia (hybrid ticketing/ loyalty/payments).

## Conclusion

In summary, biometrics is now a must-have technology that enables convenient, secure and touchless payments across all physical and digital payment channels – not just mobile. Supporting this, the Covid-19 pandemic has had a huge impact on the use of biometrics, with people increasingly using online services and many individuals making payments online for the first time. Reservations about using shared PIN-Pads and POS devices in physical locations has resulted in an acceleration of mobile wallet usage and made biometric payment cards even more attractive to consumers.

[1] Goode Intelligence Biometric Payments market technology analysis, adoption strategies and forecasts 2021-2026: https://www.goodeintelligence.com/report/biometrics-payments-market-technology-analysis-adoption-strategies-and-forecasts-2021-2026/

[2] https://worldpay.globalpaymentsreport.com/en/

[3] https://worldpay.globalpaymentsreport.com/en/

# SPEAKERS

**Tony Allen, CEO, Age Check Certification Scheme (ACCS)**
Tony is a Chartered Trading Standards Practitioner with specialism in the protection of children from harm through access to age restricted goods, content and services. He is Chief Executive of the Age Check Certification Scheme, a UKAS accredited and ICO approved conformity assessment service. He is also Chair of the BSI Standards Committee developing a new ISO for Age Assurance Systems and the Chair of the UK Government's Expert Panel on Age Restrictions.

**Rajan Barara, Product Management Director, Identity as a Service, Entrust**
Rajan Barara is the Product Management Director for Identity as a Service, Entrust's global cloud identity business segment. Prior to joining Entrust in 2016, Rajan held various leadership positions with Cloud and Managed Services companies. Rajan holds an MSc in Data Engineering from Keele University in the UK and a B.E. in Electronics and Communication Engineering from Delhi College of Engineering.

**Jordan Blake, VP Products, BehavioSec**
Jordan's role as VP of Products drives the vision, growth, and quality of BehavioSec`s solutions, and client satisfaction with them. His 20-year career in product management, cybersecurity, and cybersafety has spanned work with global industry leaders like IBM and Symantec. Most recently as Director of Product Management at Symantec, he led product efforts to integrate LifeLock after its $2.3 billion acquisition. He previously led the early product management function at FireEye (FEYE), leading to a multibillion-dollar IPO. Jordan holds a B.S. from the University of Waterloo, Canada and currently resides in the San Francisco Bay Area.

**Chris Burt, Managing Editor, Biometric Update**
Chris Burt is the managing editor of Biometric Update. He has also written nonfiction about web hosting, dramatic arts, sports culture, and fantasy basketball, as well as fiction about a doomed astronaut. He lives in Toronto.

**Nicole Gibbs, Member Relationship Manager, Cifas**
Nicole Gibbs has worked at Cifas for over seven years and has been a Member Relationship Manager within the Member Experience team for five of those. She currently manages over 100 members across a wide range of sectors. Before working at Cifas Nicole's previous experience also covered various sectors, including banking, mortgages and hire purchase, having worked in operational fraud roles at both Santander and rent-to own retailer BrightHouse. When she is not enthusiastically talking about all things fraud you will probably find her with her head in a book.

**Alan Goode, CEO, Chief Analyst and Founder of Goode Intelligence**
Alan Goode is the CEO, Chief Analyst and Founder of Goode Intelligence, a world-leading identity and biometrics research and consulting organisation founded in 2007 and based in London. With 13 years of research and analysis experience and 17 years of senior management and technology consultancy including strategy and deployment, Alan is an expert in biometrics, authentication/identity, fraud management and cyber security. His previous roles include Head of Information Security at T-Mobile UK, Security Practice Manager at Atos Origin, Head of Digital Security at De La Rue Identity Systems (including biometric passports) and Security Analyst for Citibank (Payments).

**Michelle Goode, COO, Goode Intelligence**
Michelle Goode is responsible for business planning, operational management and communications at Goode Intelligence and is an established speaker and moderator. Previously, Michelle was a key communications leader for leading financial and technology organisations with senior positions at the Pension Protection Fund, 3M and GEC/Marconi. She is an Associate of King's College, London University where she graduated from with a BA (Hons) degree and holds a Post Graduate Diploma from the University of Warwick in International Engineering Management.

**José Luis Huertas, CEO, Mobbeel**
I'm a passionate software developer, architect (one of the kind that thinks if you are unwilling to be hands-on, you should keep your hands off), entrepreneur and CEO at Mobbeel. I love to learn new things and I'm always looking for new ways to go out of my comfort zone because challenges make me grow. I have a slight disrespect for the limits of what most people consider possible. My goal is to create software that makes people's life at least a tiny bit better. At Mobbeel, we are developing easy-to-use, highly secure, mobile biometric solutions that everybody will be able to use anytime and anywhere.

**Neil Jordan, Member Relationship Manager, Cifas**
Neil Jordan joined Cifas as a Member Relationship Manager in its Member Experience team in July 2020. Neil's previous experience is across various sectors notably spending nearly nine years, mostly in fraud roles, with the HSBC Group before taking a role with the City of London Police working in the National Fraud Intelligence Bureau (NFIB) first as a Crime Reviewer and then as a Senior Analyst. After over four years with the NFIB, Neil moved to a Fraud Strategy Manager role with the rent-to-own retailer BrightHouse, with responsibility for all things Fraud (Internal and External) and some wider Financial Crime, whilst managing a team of Fraud Investigators and a Fraud Analyst. It is from BrightHouse that Neil joined Cifas and he now manages members across a number of sectors with a particular focus on our Retail and Onboarding/Vetting Specialist members and a strong interest in Internal Fraud.

**Ramesh Kesanupalli, CEO, Digital Trust Networks & Founder, FIDO Alliance**
Ramesh Kesanupalli is currently the CEO of Digital Trust Networks. Mr. Kesanupalli is also the co-founder of ADI Association, a non-profit industry organization working with global companies to define the Accountable Digital Identity Architecture (ADIA). Prior to this, Mr. Kesanupalli was the founder of FIDO Alliance, a standards body setting a global standard for Authentication. He has served at the C level in several organizations.

# SPEAKERS

**Dr. Rolf Lindemann, VP Products, Nok Nok Labs**

Dr. Rolf Lindemann is responsible for the development and strategy of the company's products and solutions. Bringing more than 20 years of experience in product management, R&D and operations from the IT security industry, he has deep knowledge of security markets and technologies. Dr. Lindemann is one of the leading experts in FIDO and has been a frequent speaker at industry events. Prior to Nok Nok Labs, Rolf Lindemann worked as Senior Director Product Management at Symantec where he was responsible for research and product strategy on device authentication in smart grids and mobile networks. Before Symantec's acquisition of TC TrustCenter, he was Executive Director Product Strategy at TC TrustCenter GmbH. Named to that position in 2009 he was responsible for analyzing market trends and aligning the overall product portfolio to new market opportunities. Dr. Lindemann received his PhD from the Technical University in Hamburg-Harburg and holds a master's degree in electrical engineering.

**Jenn Markey, Product Marketing Director, Identity, Entrust**

Jenn Markey leads product marketing for Entrust's Identity business segment. She is responsible for helping to build the company's profile in the identity and access management (IAM) market, customer footprint, and strategic business value. Jenn brings 25+ years of high tech sector experience to her current position, predominantly in senior marketing and product management roles across many different technology domains including security, SaaS, IoT, telecom, and semiconductors.

**Chris Rallis, Head of Fraud & Authentication, BehavioSec**

Chris is a Fraud & Authentication SME with over 15 years of experience fighting financial crimes. Chris spent the first 10 years of his career working in operational and strategy roles at Bank of America, JPMC, Citi, and TD Bank. For over the past 5 years, Chris has taken his practitioner experience into the start-up world of anti-fraud and authentication, working with Pindrop and BioCatch prior to joining BehavioSec. As Head of Fraud & Authentication at BehavioSec, Chris partners with customers, globally, to mitigate emerging fraud threats, reduce user friction, and enable digital transformation using behavioral biometrics.

## GOODE INTELLIGENCE VISIONARY AWARD RECIPIENTS

Visionary for Authentication 2021
**Phillip Dunkelberger**

Visionary for Biometrics 2021
**Dr. Neil Costigan**

Visionary for Identity 2021
**Emma Lindley**

# Guest article

## Did you know? A passwordless experience isn't necessarily passwordless

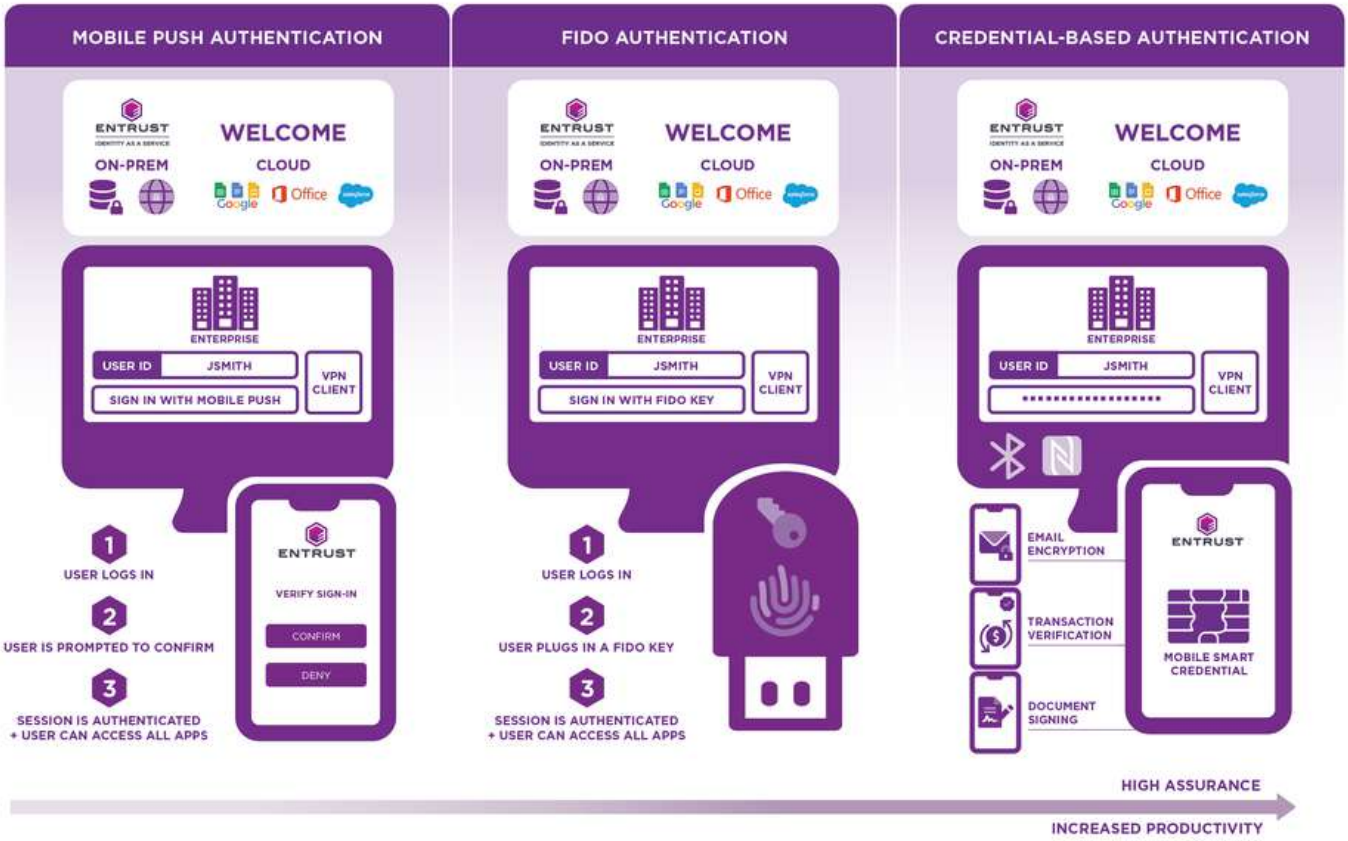
***Jenn Markey,***
***Product Marketing Director***
***Identity Business Unit, Entrust***

Nobody likes passwords. From an IT perspective, passwords are notoriously insecure with compromised credentials accounting for 81 percent of all data breaches. As well, passwords take precious time, money, and resources to manage. From a user perspective, passwords are annoying. The average American internet user has 150+ accounts requiring passwords, far beyond the capacity of human memory promoting bad habits like password reuse and recycling. And poor password hygiene further fuels the security risk. Plus, people are simply tired of being continually prompted to enter their credentials to access different apps and sites.

With the dual promise of improved security and a vastly better user experience, it's no surprise there's a lot of interest in going passwordless. However, not all passwordless solutions are equal. One of the biggest things to note is that providing a passwordless experience and removing the password are not necessarily the same thing. For example, mobile push authentication is a widely adopted passwordless implementation that still backs to a password. Great passwordless user experience, but it does not address the security vulnerability of relying on passwords. While this may be sufficient for consumer use cases, it definitely leaves a lot to be desired for high assurance workforce use cases. An alternate method to authenticate is to configure a QR (Quick Response) code that permits a registered device to scan a machine-readable code for verifying user identity. It is a contactless authentication method that offers a good balance between security and usability without affecting user privacy.

With asymmetric encryption, FIDO provides a more secure passwordless experience than mobile push, but still relies on a password for initial registration and the password continues to exist post key generation. As well, FIDO keys work on the basis of possession, so if I have someone else's FIDO token/key, then I can assume that person's identity. FIDO does not prove the identity of the person holding the key. There are some FIDO keys that are biometric enabled, but these are few and far between given challenges to easily imprint biometrics onto a FIDO key. Plus, FIDO does not address typical workforce use cases like email signing and encryption, digital document signing, and file encryption. Then there is the IT administrative overhead of registering and managing all those FIDO authenticators.

Enter credential-based passwordless authentication which removes the physical password entirely, replacing it with a digital certificate. The certificate is provisioned onto the worker's mobile device transforming it into their trusted digital identity. When the phone is unlocked via the user's biometrics (i.e. fingerprint or facial recognition) and in close proximity of their workstation, they




are automatically logged into the workstation and able to access all of their applications without having to reauthenticate themselves. When the worker walks away with their phone, they are automatically signed out of any apps they were using and logged out of their workstation. Plus, with a PKI-credentials based solution not only can the identity of the user be validated by a public CA, but users are also able to send signed and encrypted emails, digitally sign documents and encrypt files. A truly passwordless solution for improved security, reduced costs, and happier more productive users.

Simply put, there is more to passwordless authentication than just removing the password – from security and configuration to the experience you deliver your users. Credential-based passwordless authentication combined with adaptive security provides a strong foundation to realize a Zero Trust approach.

**www.entrust.com**

ENTRUST

# The biometrics journey to support a real digital identity

When Woodrow Wilson Bledsoe began the development of the first facial recognition solutions in the 1970s, he probably never imagined the great evolution that technology would undergo, the multitude of applications it has today and its tremendous impact on society. And that the development of all kinds of biometric techniques, both physical and behavioural trait analysis, has been enormous, especially in recent years thanks to the development of deep learning technologies and neural networks.

Without going any further, in 2009 we were pioneers worldwide in developing the first solution capable of iris recognition with mobile devices (those available at that time!), ahead of companies such as Google (2011: Face Unlock) or Apple (2013: Touch ID, 2017: FaceID).

But we soon realized the challenges presented by biometric recognition technologies in mobile environments, where using a single biometric trait as an authentication mechanism presents limitations caused by hardware, environmental conditions (light, noise, etc.) and many others. A single biometric to authenticate users is no longer enough.

And since no biometric technology is better than another, we were continually incorporating new features by which to identify people (voice, face, signature or fingerprint); embracing multibiometry as the holy grail.

Still, this increasingly robust development presented significant security issues in the face of increasingly ingenious phishing attacks. It is no longer enough to find matches between a sample and its biometric pattern, in addition you have to verify that there is a real person carrying out the process and not a cybercriminal who wants to impersonate your identity. It is necessary to incorporate life detection tests into the biometric process to prevent attacks with photos, videos or masks.

At this point, surely our colleagues in the R&D department could rest easy by evolving active and passive liveness detection techniques or adding new behavioural biometrics to the multi-biometric stack. But nothing could be further from the truth. We quickly realized that there were more weak links in the chain that needed to be reinforced... What if you want to use biometrics to record and process a new user? How do you reliably guarantee the identity of a person accessing your system for the first time with their biometrics?

> "How do we know that those biometric templates identify me and not Donald Duck?

We can compare two biometric templates and know that they belong to the same individual, but if at the time of registering the biometrics my identity is not verified, how do we know that those biometric templates identify me and not Donald Duck?

Currently we can use technologies that allow verification of the identity of a person in a digital onboarding process by scanning a real identity document and verifying their identity with facial biometrics.

In short, if we want to use biometrics to have a real, secure and powerful digital identity, we have to use more than one biometric factor, along with liveness detection techniques and verify the identity of the user at the time of registration with an identity document. In this way we can use biometrics for countless uses and applications, including document signing processes, adding or eliminating layers of authentication depending on the risk profile of the client or the transaction that is going to be carried out.

No one should suffer fraud. We understand that feeling and that is why we have developed a robust multibiometry verifying identity in onboarding as a way to make the world a safer place and enables you to carry out digital transactions with the same confidence as in person.

mobbeel

mobbeel

## Identification solutions for each stage of the relationship with your customers

From the registration process, through the digital signature to authentication when necessary with any of our identity verification solutions:

Incorporate your new digital clients through our eKYC / AML technology in seconds, scanning an identity document and verifying the identity of the holder with facial biometrics. Next, formalize your contractual relationship with the company with our advanced electronic signature and finally, authenticate your users every time they access your system or authorize a transaction with facial, voice, fingerprint or signature recognition. More info: *www.mobbeel.com | info@mobbel.com*.

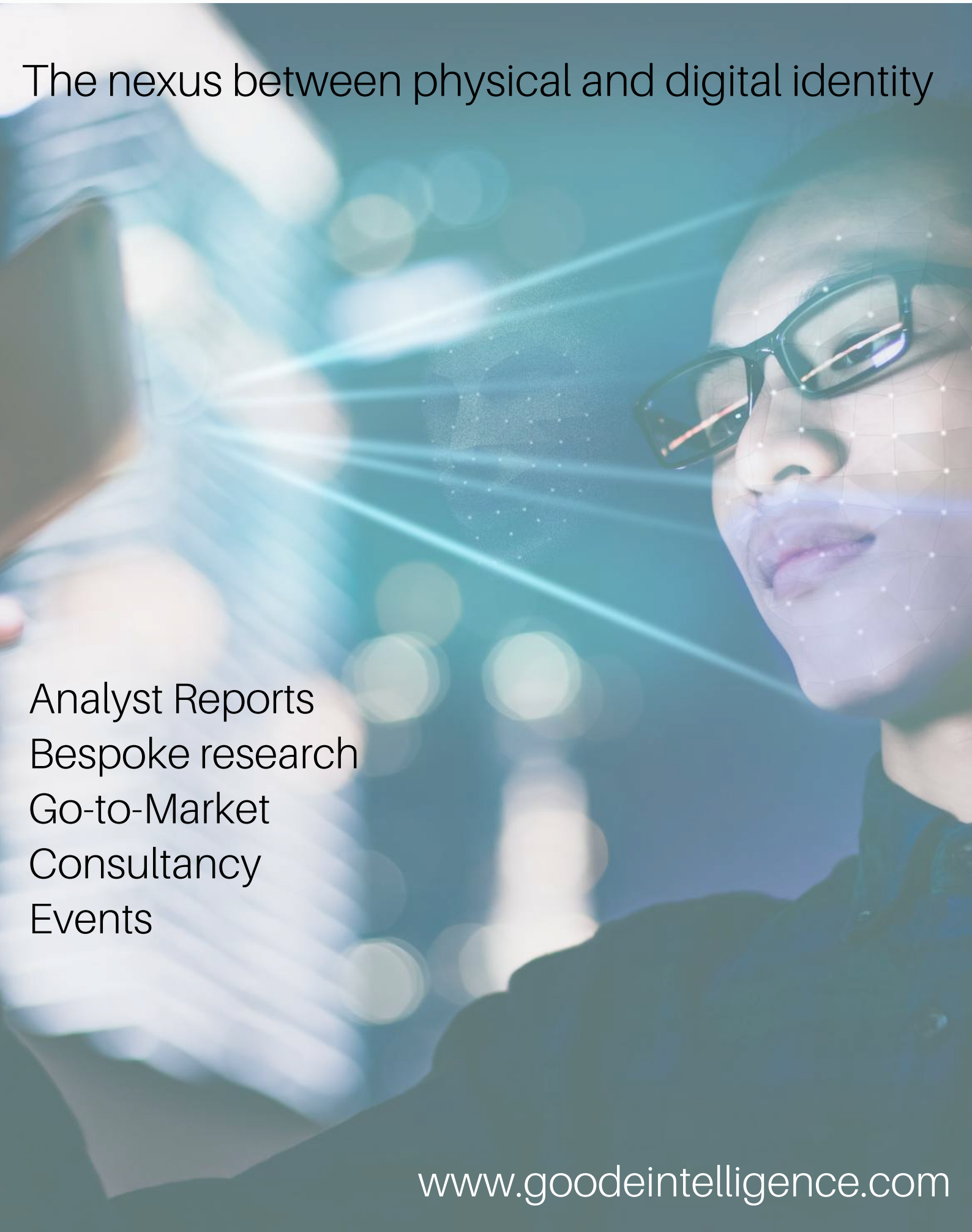

mobbID


mobbScan

mobbSign

GOODE INTELLIGENCE
YOUR PARTNER FOR BUSINESS RESEARCH & ANALYSIS

# The nexus between physical and digital identity



Analyst Reports
Bespoke research
Go-to-Market
Consultancy
Events

www.goodeintelligence.com

# DIGITAL TRUST WORLD:

## COMBATING SOPHISTICATED DIGITAL FRAUD ATTACKS IN THE MODERN ERA UTILIZING BEHAVIORAL BIOMETRICS

BehavioSec is excited to participate in this year's Digital Trust World conference, where the company's head of fraud and authentication, Chris Ralis and vice president of products, Jordan Blake will discuss how behavioral biometrics can play an even greater role in combating the growing threat of digital fraud. Their discussion is entitled, "Behavioral Biometrics: A versatile technology for fraud detection and authentication."

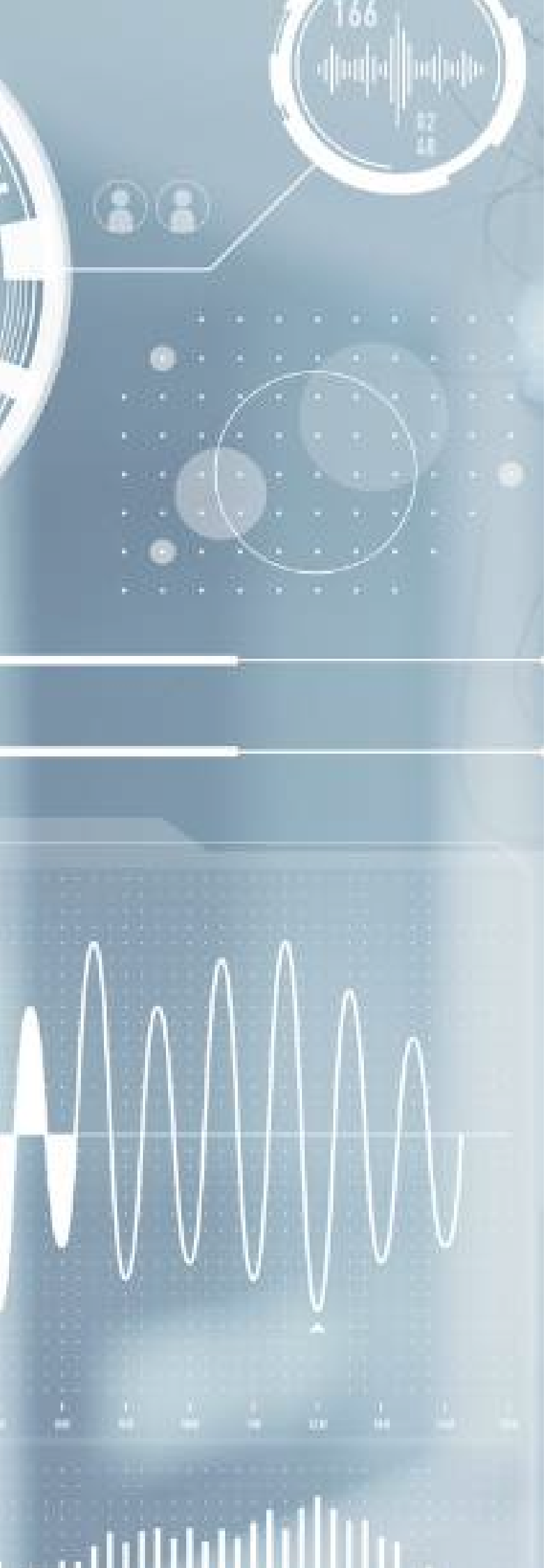
This is an important discussion to have at this year's conference amid the accelerated digital transformation so many companies large and small have experienced over the last 20 months in response to the global pandemic. Workplaces have evolved, so too has the supply chain and business operations.

With that has come an expanded digital risk environment where there's more potential for fraud to be committed - within the company enterprise or elements associated with it. It requires companies to reimagine the way they protect digital identities and authenticate. Gone are the days when a single passcode or fingerprint at login are enough to protect users throughout their digital journeys.

BehavioSec has been partnering with companies all over the globe to address this requirement. The company is the industry pioneer and technology leader for behavioral biometrics and continuous authentication, safeguarding millions of users and billions of transactions today. Its technology is deployed across Global 2000 companies to dramatically reduce fraud, friction, threat, and theft.

### How does the technology work?

BehavioSec uses behavioral biometrics to turn authentication into an invisible, continuous process while maintaining security, privacy and compliance. Its platform does this by silently analyzing patterns in physical behaviors like typing, swiping and mouse movement to verify and protect people online.



More companies are embracing behavioral biometrics to combat digital fraud but are needing capabilities and support that ensure a seamless user experience and scale with their compliance and business needs. Recently, BehavioSec unveiled a new SaaS-version of the company's BehavioSense platform - the market's first to offer comprehensive behavioral biometrics for multi-factor authentication in a lightweight, self-service form factor. Unlike other SaaS-based solutions that may specialize in just web interfaces or typing, this new platform brings the company's deep insights across device types and human interaction to identify unique humans during the authentication process.

A company's digital risk environment will continue to evolve, requiring a modern approach to authentication for modern times. Tune in to this session to learn how BehavioSec offers the versatile technology that is needed to combat the ever-changing world of digital fraud attacks.

BehavioSec®

# Continuous invisible security

Protect against

New account fraud
Account takeovers
Social engineering

→ Invisible multifactor authentication
Frictionless user experience
Continuous authentication

BehavioSec®
Better Authentication. Better Experience.

535 Mission St, 14th Floor • San Francisco CA 94105 • +1 (833) 248-6732 • behaviosec.com

# Our thanks to all our Sponsors and Partners for DIGITAL TRUST WORLD 2021

## SPONSORS

BehavioSec is the industry pioneer and technology leader for behavioral biometrics and continuous authentication, safeguarding millions of users and billions of transactions today.

Deployed across Global 2000 companies to dramatically reduce fraud, friction, threat and theft, BehavioSec verifies and protects human digital identities by understanding how we uniquely type and swipe across our ever-changing devices. Whether used in the Cloud or on-premises, BehavioSec delivers the superior user experience, precision, and scale needed by organizations to keep customers engaged while catching evasive, real-time attacks other solutions miss.

Founded in the Nordics in 2008 out of groundbreaking research, industry recognized BehavioSec partners with market leaders and organizations like DARPA, and has earned investment from top firms like Forgepoint Capital, Cisco, ABN AMRO, Conor Ventures, and Octopus Ventures. Headquartered in San Francisco, CA with offices worldwide, BehavioSec is ready to help you reduce risk, improve compliance and digitally transform your distributed workforce and customer experience.

Entrust keeps the world moving safely by enabling trusted identities, payments and data protection. Today more than ever, people demand seamless, secure experiences, whether they're crossing borders, making a purchase, accessing e-government services or logging into corporate networks. Entrust offers an unmatched breadth of digital security and credential issuance solutions at the very heart of all these interactions. With more than 2,500 colleagues, a network of global partners, and customers in over 150 countries, it's no wonder the world's most entrusted organizations trust us. For more information, visit **www.entrust.com**

Founded in 2009, at Mobbeel we develop solutions to identify users in a convenient and secure way. We have more than 12 years of experience with clients from multiple sectors in more than 30 countries and millions of verified identities and we have developed our own technology to be flexible and cover all your needs whatever your requirements. Furthermore, we are pioneers in biometric recognition technology for mobile devices without the need for specific hardware, but above all, we are passionate about our products and keep working and innovating to achieve excellence.

Nok Nok is a trusted leader in passwordless consumer authentication to the world's largest organizations. Delivering the most innovative authentication solutions in the market today, Nok Nok empowers global organizations to improve the user experience to access digital services, while meeting the most advanced privacy and regulatory requirements. The Nok Nok™ S3 Authentication Suite integrates into existing security environments to deliver a proven, cost-effective, future-proof and standards-based passwordless consumer authentication solution. Headquartered in Silicon Valley, California, the company has delivered unique inventions and innovations that are protected by a robust global patent portfolio. As a founder of the FIDO Alliance and an inventor of FIDO specifications, Nok Nok is the expert in deploying standards-based authentication, and its industry leading customers and partners include BBVA, DDS, Inc., Ericsson, Fujitsu Limited, Hitachi, Intuit, Lenovo, MTRIX GmbH, NTT DATA, NTT DOCOMO, OneSpan, SoftBank, T-Mobile and Verizon. For more information, visit www.noknok.com

## MEDIA PARTNER

BiometricUpdate.com is the leading news property that publishes shareable breaking news, analysis, and research about the global biometrics market.

# PARTNERS

The Age Check Certification Scheme (ACCS) is a UKAS accredited and ICO approved conformity assessment service. ACCS checks that identity and age check systems work. It undertakes independent and impartial assessment of all approaches to ID and age assurance, including undertaking mystery shopping, analysing the efficacy of biometric processes, carrying out presentation attack detection (anti-spoofing) and undertaking a wide range of assurance testing or services in its purpose built and accredited test studio.

Cifas is the UK's fraud prevention community. We lead the fight against fraud by sharing data, intelligence and learning. Our community is drawn from all sectors, working together to stop fraud.

Digital identity is broken. It's time to fix it. Digital Trust Networks gives ownership of identity back to the individual to eliminate identity fraud and protect privacy. Digital Trust's DTX® platform creates a strong identity for life for every human being, bio-metrically bound to only that person without the need for passwords. No one else can claim that identity or access that person's information without their consent. DTX® is the first commercial implementation of the open framework for Accountable Digital Identity.

The FIDO (Fast IDentity Online) Alliance, www.fidoalliance.org, was formed in July 2012 to address the lack of interoperability among strong authentication technologies, and remedy the problems users face with creating and remembering multiple usernames and passwords. The FIDO Alliance is changing the nature of authentication with standards for simpler, stronger authentication that define an open, scalable, interoperable set of mechanisms that reduce reliance on passwords. FIDO Authentication is stronger, private, and easier to use when authenticating to online services.