HOW FINTECHS CAN TACKLE MOBILE FRAUD

DURING COVID-19 AND BEYOND

TMTANALYSIS

Contributions from

cifas Leaders in fraud prevention

FRACTAL LABS

HUBUC

Kalgera

ONE WORLD IDENTITY

Executive Summary

On the 17th of November 2020 TMT Analysis brought together a roundtable of leading experts in mobile identity, mobile fraud and fintech to discuss the rise in mobile fraud and what could be done to tackle it. This Whitepaper is produced using the comments of all the participants and their thoughts on the central question '**How fintechs can tackle mobile fraud during COVID-19 and beyond?**'

The roundtable was moderated by **Sharon Kimathi**, Editor at **FinTech Futures**, and featured:

John Wilkinson, CEO at **TMT Analysis**

Mark Courtney, Chief Product Officer at **Cifas**

Simeon Beal, Director, Advisory Services at **One World Identity**

Chryssi Chorafa, Chief Operating Officer at **Kalgera**

Nicholas Heller, CEO of **Fractal Labs**

Ignacio Javierre, Co-Founder of **Hubuc**

Lionel Tapiero, Head of Strategy and Business Development for **Otomo**

> Identity fraud is still the biggest type of fraud we see
> Mark Courtney, Cifas.

There is no doubt that fraud increased significantly in 2020. According to Cifas, the UK's leading anti-fraud organisation, facility takeovers (where a fraudster gains access to the accounts of innocent victims and then uses that access for their own benefit), increased by 34% in 2020. Mobile and telecoms fraud accounted for over half of those cases recorded.

This increase in online fraud is because of changes in behaviour brought about by the impact of Covid-19. The amount of mobile and online activity in terms of account openings per day, whether that be a bank account or an e-commerce profile, has spiked dramatically over the past year.

What is obvious is that tackling this problem is problematic for many organisations globally who are facing challenges setting up or establishing a suitable anti-fraud mechanism. Companies are either taking one of two routes – assuming everyone is bad and letting trusted third parties in, or assuming everyone is good and trying to weed out the bad people.

The public v private debate too in terms of identity management and fraud reduction was discussed by all our participants, with the main issue in terms of who should take the lead, the government or private enterprise? According to Simeon Beal from One World Identity countries where there is good collaboration between public and private such as in Singapore, the Nordics, or even Canada which is bringing together institutions like 'Verified Me', telecoms companies, the banks and government and is seeing great success in terms of fraud reduction and successful identity verification.

All the participants agreed that globally there needs to be standardisation and harmonisation in terms of identity management, KYC and onboarding of customers. Many noted the complexity of complying with local and regional rules around privacy, identity and anti-fraud checks. For customers, the most important aspects of any identity check are its ease of use and whether it is compliant with the rules. Many participants want to see a better experience for customers than what we have now, focusing on how we can better serve and retain customers, whilst balancing risk concerns and regulations.

The vision for all was that more sectors will collaborate in sharing data, not only from the banking sector, but transactional data, mortgages, lending etc. Mobile companies too could equally be part of this more open data sharing.

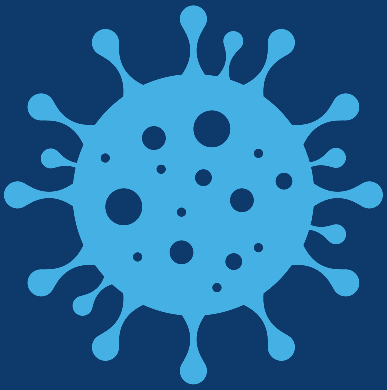
In summary I will leave you with the words of Simeon Beal again from One World Identity. "If Covid never hit, I think that mobile fraud and digital identity, at least in most of our experiences, would be something that was on the fringes, and it's now something you can no longer ignore. I think we finally have a lot more motivation behind us for that. Hopefully, people are just preparing for it in the future, and we can start having more inclusive and sustainable infrastructures."

John Wilkinson, CEO, TMT Analysis Ltd.

97% of Millennials use mobile banking

91% of Gen Xers use mobile banking

Business Insider



COVID-19 has further driven up adoption of mobile banking. The U.S. FBI notes a **50% surge in mobile banking** since the start of 2020 and predicts that fraudsters will capitalize on this increase by stealing credentials through fake banking apps and app-based trojans

Pre-COVID mobile commerce of global ecommerce sales was expected to grow from **48%** to **70%** by 2022.

McKinsey

64% of respondents have faced payment fraud,

63% have battled fake accounts,

42% have had their account taken over, and

55% are fighting fake content.

Sift survey on digital trust & safety

What is fraud?

The TMT Analysis roundtable started off by unpacking the key elements of fraud. The legal definition of fraud is the "*intentional deception to secure unfair or unlawful gain, or to deprive a victim of a legal right*". The means of committing this crime continues to radically change throughout the years – especially after significant technological developments – from the internet and laptops, to smartphones and artificial intelligence (AI), the means of adapting to new tools is proving to be seamless for fraudsters.

> **Fraud takes place when the person is not who they say they are and the objective is to misappropriate funds, so using a fake identity and pulling the capital out of that account to a different one – stealing money by stealing identity first.**
> Lionel Tapiero, Otomo

Mark Courtney, chief product officer at Cifas, chooses to highlight two types of fraud. "First-party fraud – that person is committing fraud using their own identity. Then you have third-party fraud – pretending or acting on behalf of a real identity in order to commit fraud."

Simeon Beal, director for advisory services at One World Identity, explains it as "the abuse of a platform from any malicious user, be it for the transfer of capital or disproportionate gain". He points out that the framework for setting up anti-fraud mechanisms in one's platform is challenging as "you either take the position assuming everyone is bad and letting trusted third-parties in, or assuming everyone is good and trying to weed out the bad people".

Tapiero sees that the increase in the amount of activity and amount of account opening per day has spiked, both in robo-advisory or digital bank account opening, and this brings its own set of compliance challenges. "We've seen tremendous success in account opening this year, so it's really hard to keep pace if you have any sort of manual review or, to Simeon's point, 'are you letting everybody in and phasing them off over time?' and, these strategies become paramount and put a lot of pressure on the organisation, so if there's anything that's manual you are now probably having a queue, and you are not able to hit your objectives."

He notes that the compliance manager he had put in place went through a manual review, so they implemented letting people in and then conducting a review, which he admits to being incredibly hard.

Increase in fraud amid COVID-19

Cifas has seen an increase in facility takeovers (where a fraudster gains access to the accounts of innocent victims and then uses that access for their own benefit), with a 34% increase year-on-year. Courtney adds that telecoms accounts for over half of those cases recorded, but SIM swaps (a type of account takeover fraud that generally targets a weakness in two-factor authentication) made up only 5% of that number. "Identity fraud is still the biggest type of fraud we see, but facility takeovers are definitely on the rise," says Courtney. He believes that fraudsters, or those that are conducting fraudulent behaviour, are transforming their usual activities. "Adopting real identities or getting the real person to commit the fraud, is now more common than it was". According to the Insurance Identity Institute, identity theft and fraud has been on the rise because "criminals are becoming adept at foiling authentication processes, particularly mobile phone account takeovers."

Chryssi Chorafa, chief operating officer at Kalgera, highlights the ramifications of fraudulent activity on vulnerable customers. "We started observing people that have got some type of cognitive impairment, but then that extended as well, and what we have seen from the past few months – especially since the pandemic – is an increase of fraud from couriers, Amazon deliveries or volunteers trying to defraud people who have a lower capability of judgement on whether a person is approaching them for 'good' or 'bad' means." Chorafa notes that those same people's experience throughout the year includes social engineering scams, and that "they are so much more vulnerable during this pandemic, as they do not have that support either from families or friends, and these types of events have increased".

Courtney finds that the definition of what counts as "vulnerable" has changed due to the pandemic. He explains that it now includes "people losing their jobs, people looking for money, as vulnerability changes day-to-day, and we often think of the vulnerable as a very small percentage of society, but that changes and is more transient than it ever was right now."

> “Avoid being the lowest common denominator”
> Simeon Beal, One World Identity.

"Fraudsters are trying to take advantage of people in a longer-term span," says Beal. He cites the Federal Bureau of Investigations (FBI) crime stats report, which shows how fraudsters are waiting for a longer period to gain more financial information to make that one big attack and take as much as possible at once. This has been a change of behaviour that One World Identity have seen over time. His one key takeaway for anyone to avoid being targeted by fraudsters is to "avoid being the lowest common denominator" and use a password-manager to be above the baseline, as only 18% of Americans use password managers. Other points he suggests are using email filters, not re-using passwords and limiting the number of services a person uses.

“What we’re talking about here is primarily a lack of education around the understanding of some the basic fundamentals in security and privacy, especially among the vulnerable”

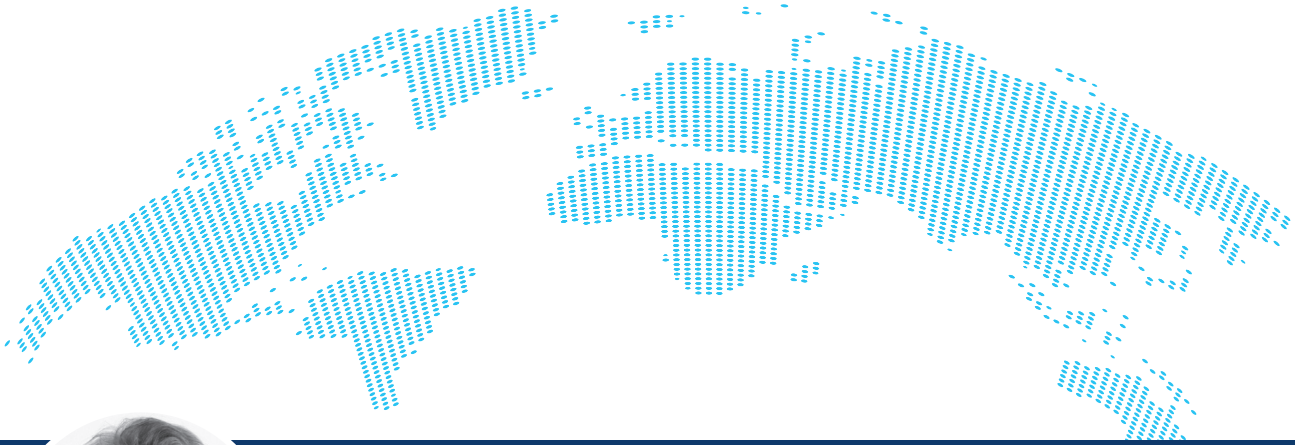
Nicholas Heller, CEO and founder of Fractal Labs.

The internet learning curve

John Wilkinson, CEO at TMT Analysis, acknowledges that some of these problems are more of an “educational and cultural exercise for the next generation to deal with”. Wilkinson finds that “we are reaping what we have sown in the internet for the last couple of generations”.

He adds: “If you look at account opening, a lot of straight forward low-friction checks can really help a lot of organisations and any kind of e-commerce business. I think one of the problems with it is that it’s not ingrained in our internet DNA. Most of us, people younger than me even, are used to social networking and email and all of these technologies which are ultimately either pseudonyms or anon friendly, which are profoundly non-secure in their absolute nature – Twitter is probably the best example.”

He explains that the anonymous ability to contribute or play a part in the internet is really quite ingrained. Creating an identity process that consumers expect in the internet is a long-term challenge, and anyone in the fintech/ banking space will ultimately suffer from that because it will be a long learning curve for the customers. “I think low friction account opening type opportunities and serious fraud questions need accounting as well, but making the internet a more trusted and secure place for lots of people via secure account opening is where there’ll be a real revolutionary quality of service via the internet.”



“If you look at account opening, a lot of straight forward low-friction checks can really help a lot of organisations and any kind of e-commerce business.”

John Wilkinson, TMT Analysis

Open banking's role in driving the change

> “The UK has advanced a lot in terms of open banking and there’s a lot of data available for services to be built to recognise a specific ID for a phone, or email, and creating that digital identity for that user.”
> Lionel Tapiero, Otomo

Wilkinson believes initiatives like open banking will really help drive this change. Tapiero seconds that, drawing on open banking comparisons between the UK and the US. “The UK has advanced a lot in terms of open banking and there’s a lot of data available for services to be built to recognise a specific ID for a phone, or email, and creating that digital identity for that user, then assigning a risk to all of them and using intelligence to determine whether or not the flow of the information is a safe account to open. But, of course, that wouldn't have been available five or 10 years ago.” Tapiero’s main concern is that this data would have been siloed in one bank and another bank and there would have been no data lake to look at or interpret the information for the purpose of opening an account or monitoring.

Chorafa adds her perspective on open banking, focusing the conversation around the importance of awareness and education when thinking about friction vs fraud prevention, especially for disabled customers. “I think there's more work to be done on that and educating the end consumer.” She notes that Kalgera has been working on creating a personal financial management tool over the past year. “We found out that it's pretty hard to onboard a customer who has different vulnerabilities, especially ones that were not that tech savvy.” She thinks this area of financial management still has a lot of work to do, as there are more things that have to be included. “The journey and the account can be open to facilitate for those people who have, for example, some type of disability or who are visually impaired or have some hearing impairment and the structure of the code might need to embed voice messaging to text and all of that.” She concludes that although this area requires a lot of attention to really make a difference, that it is still quite an exciting time as financial services can actually implement more tools to facilitate vulnerable people.

Mobile payments infrastructure and fraud

> “Firms can see the state of the SIM and the phone number and verify – in real time – whether or not the user of the number is the same as the onboarding user identity that’s been entered.”
> John Wilkinson, TMT Analysis

Wilkinson has seen firms in the mobile operating space launching tools within their infrastructure that focuses on customer verification and authentication. These are seen within a firm’s own client relationship management (CRM) or application programme interface (APIs) tool. “Firms can see the state of the SIM and the phone number and verify – in real time – whether or not the user of the number is the same as the onboarding user identity that's been entered.”

He believes this is a positive development in detecting fraudulent accounts, as it can give a warning if there's anything suspicious about a transaction, especially for low friction e-commerce and “reassure that the onboarding data is correct via a KYC match-type infrastructure”. He draws on the type of fraud that Courtney mentioned earlier – SIM swap fraud – particularly because of the prevalence of SMS two-factor authentication.

“There needs to be more rigid checks on the validity of the number and the SIM, and we're doing those kinds of checks,” adds Wilkinson.

Wilkinson hopes to see mass market adoption of this type of tool in social networking players, so mobile use will be quicker and simpler than it is for financial products. “I think there's a lot of use of mobile data, which can really help at the low friction e-commerce – not completely secure – end of the dynamic.” He believes this is the type of area TMT Analysis can prove to be useful, particularly in the mobile identity spaces, since everyone has a smartphone. “The mobile number is quite a good proxy for your identity as well, because it sits in your pocket.”

But Heller thinks that the mobile number is just one component for verification and fraud prevention, as authentication is table stakes that's been around for over a decade, if not more, so everyone should be using two-step authentication for everything. “I think the great part about mobile and mobile computing is that we've seen it grow up and evolve and change dramatically. The mobile is a unique device because it's a bionic device. It has eyes, it can see, you can hear it can speak, you can touch it.”

He draws from his experience in his previous roles where he tried to acquire a company that could identify smell, using only the device. “Unfortunately, there were really only focused on the military, but we thought that, at Google, it would be a great addition to Android where then you had a full bionic device.” Heller’s point harks back to the application of the Second Payment Services Directive (PSD2) and its strong customer authentication (SCA) requirement. “The right thing to do is what the legislation says we should be doing. That might be a password, something you have on your person like your phone number, something that's unique to you and your identity which the phone allows for like biometrics such as your face or your fingerprint. I think if you're using those three things, then you're at least one step ahead of most of the fraudsters out there.”

Beal agrees with Heller’s perspective, and wishes to see an introduction of multi-factor authentication (MFA) as a framework in the United States. But he adds that this might not be able to apply across the board because “not all phones, and not all people, have the same access to the resources to enabling MFA”.

“The next step is trying to understand fraud between the two problem sets – the creation of identity and the ability to detect fraud.” Beal believes the trick to understanding what fraud is for a firm’s user base is by tailoring a solution in order to identify behaviours in that specific geography or location. “I think managing this globally, but identifying it locally, is the key here and trying to do that in a way that is scalable is ultimately where I think we're trying to get to as an industry.”

20%

of traffic on social media in Q2' 2020 are fraudulent attacks.

89.5% of these are at the login stage; the remainder are fake account registrations. In addition...

53.3% of login attempts are fraud

Arkose Labs - VOC Surveys

19%

Increase in Mobile telecoms fraud reported to the National Fraud Database in 2020

Cifas

87%

of identity fraud in 2019 occurred through online channels

Cifas

+92%

increase in mobile banking fraud losses in 2019

UK Finance

Adaptable fraudsters

Courtney points out that despite all of these developments, one thing he sees is that "fraudsters adapt". "They find out what the problem is, they will find a way around it and they will get through the process." What he believes is important is collaboration between various organisations to combat fraud together. "Although we are UK centric, my key advice is to collaborate, not compete on fraud. This is about sharing data where you can, if there's a facility to do that, share intelligence and shared knowledge." He highlights the issues of silos, which hinders progress in this area. "What we see in the fintech space, and even in the big e-commerce world, is that people live in their silos too much. They don't share outside of that. They see it as a competitive advantage. If we're going to beat fraud, people have to sharing data outside of their own little world. It's an uncomfortable situation, but it's the right way to do it."

Additionally, he wishes to see firms within the industry adapting quicker to change. "We talk about biometrics and all that, and it is absolutely a valid thing to do. But what fraudsters have done now is they've gone out to countries where they can get a genuine document formed by biometrics and they can open an account somewhere with that." For Courtney, what might tackle this type of fraud is fast adaptation to different authentication tools. "For example, at Cifas now, we're doing facial matching against documents that have been loaded by members for fraud into the national fraud database fully. It's enough that we're seeing around 11 accounts with the same face under 11 valid identities around it." His example shows how easy it is for fraudsters to create an identity and manipulate the gaps in the system.

"My key advice is to collaborate, not compete on fraud. This is about sharing data where you can, if there's a facility to do that, share intelligence and shared knowledge."
Mark Courtney, CIFAS

The public v private debate

> I think in countries where you do see increased collaboration around Singapore, the Nordics, or even Canada, I know institutions like 'Verified Me' are coming out with trying to bring the telcos, the banks and the governments together.
>
> Simeon Beal, One World Identity.

Beal believes that collaboration between private sector and public sector has really helped with fraud management. "I think in countries where you do see increased collaboration around Singapore, the Nordics, or even Canada, I know institutions like 'Verified Me' are coming out with trying to bring the telcos, the banks and the governments together."

"I think there's an acknowledgement that competition should be around the product level and not necessarily around the identification level. Let's try to get access for everyone to these services and then we can compete above and beyond that. I think you're seeing much more successful, authentication sessions, as well as more robust and comprehensive identity practices. Places such as the US are having more competition, and we're still not entirely sure where we're figuring out whether or not we're having a national identity scheme. And private sectors are still trying to do their own thing and compete against one another. I think fraudsters see that as an opportunity to capitalise on this disunity and try to take the same problem with the same vector and apply it across different industries and including the government."

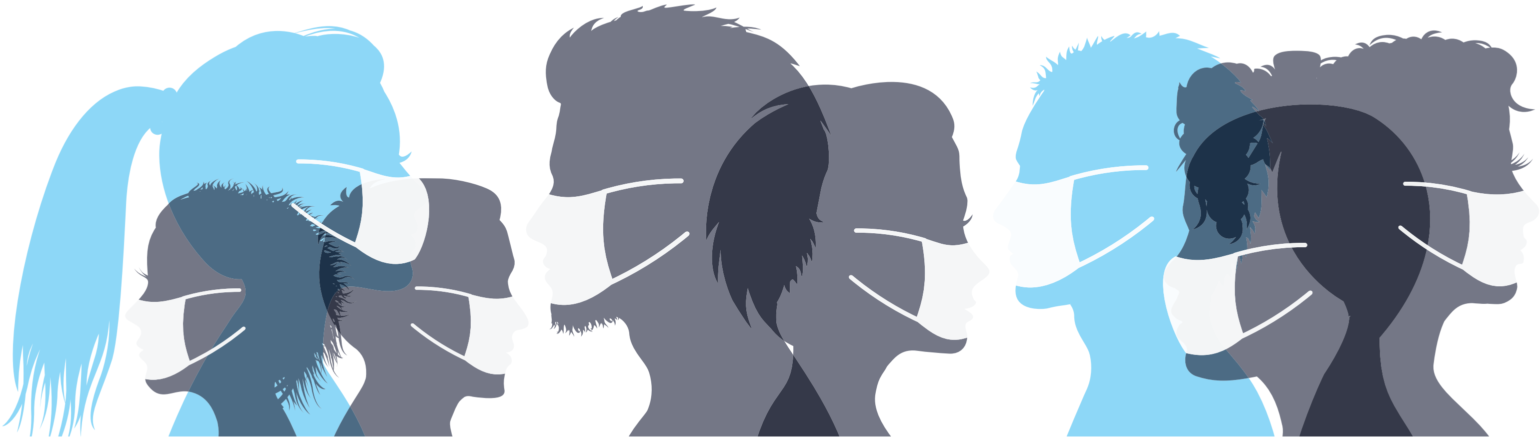
Courtney draws on the example in the UK and its handling of the track and trace app (or lackthereof) from Serco. "We're a non-for-profit and we kind of sit in the middle ground between public and private. We have specified anti-fraud organisation status in the UK, which allows us in legislation to share data between public and private sector." He has seen a prevalence in collaboration whereas it was quite one-way in the past.

Tapiero believes that another way to think about it is the speed at which a government or entity would move with respect to a problem like fraud. "I think it has to be in the hands of people that can act and can solve these problems within a framework that's reasonable. We go back to that concept of collaboration because it is the role of the government to put in place a framework, and then innovation comes within that box.

Change of behaviour during the pandemic

“The kind of behavioural analysis in life management of a customer is what I think will change a lot,” says Wilkinson. “For instance, we have a facial recognition system in my office. But all it does is just checks on the same face I was last time. There's no check against where my face might have originated from, or whether my face is attached to ‘John Wilkinson’ or not. I think that's a kind of good example of sometimes where things like biometrics obviously appear great, but ultimately, maybe aren't. I think there’s a real opportunity for in life management of customers around cyclical checks, but also around lean or dramatic spikes in behavioural change. And I think that's one kind of revolution where the data, the data kind of moving in and out, being shared, and that profiling of what a normal customer looks like to your business, can really be quite a powerful tool.”

Heller draws from his experience in the advertising industry. “Over the last 20 years, advertisers have used data in a very clever way. When you're talking about motivation, they're very motivated to drive up revenue by using as much data as they can. And let's be very clear, Google and Apple and the developers on their platforms know everything about you and your phone. By default, you have to opt out of the advertising ID that is on your phone, which basically tracks every single piece of usage, every app you use, where you've been – literally everything on your phone. I think it's really interesting if you use that in the financial services context around fraud. I think there's some interesting things you can do because you basically know that user’s behaviour.”



The future of fraud and mobile

> “The vision is that more sectors will collaborate in sharing data, not only from the banking sector, but transactional data, mortgages, lending etc. Mobile companies could equally be part of this more open data sharing and contributing with open finance.”
> Chryssi Chorafa, Kalgera

Javierre notes that the application of KYC and AML policies at each country in Europe needs greater standardisation and harmonisation. “Because we've seen that there is complexity when it comes to complying with local rules or issuing cards and opening bank accounts. For our customers, the most important thing for them is for us to be compliant with these rules.” He hopes to see a better experience for customers, focusing on how he can serve and retain his customers, whilst balancing risk concerns and regulations.

Chorafa draws the comparison with open banking and mobile data – connecting and sharing with financial services to better profile a customer. “The vision is that more sectors will collaborate in sharing data, not only from the banking sector, but transactional data, mortgages, lending etc. Mobile companies could equally be part of this more open data sharing and contributing with open finance.”

Wilkinson sees the positive effects of these challenges, adding that there is “something powerful about the new entrants in the market”. He finds that more traditional organisations might be slower or harder to move. “One would think that actually this problem can drive innovation, which can help new entrants, new technologies, new companies, do better and leave some of the dinosaurs behind. Hopefully it means the internet can stay lively and useful over time.”

Courtney closes on his main observations this year and where he sees it heading. “I think we have to be aware of what's coming. I think there’s a greater likelihood of it being the real person being convinced to commit fraud. We're seeing that with scams, we're seeing that with ‘money muling’, where people are being recruited with threats of violence or they're being recruited on social media. That's where people are heading. I don't see fraud still being massive, but we need to be aware of the perception and the methodology changing, which is on the rise.”

> “If COVID never hit, I think digital identity, at least in most of our experiences, as something that was on the fringes, is now something you can no longer ignore. I think we finally have a lot more motivation behind us for that. Hopefully people are just preparing for it in the future, and we can start having more inclusive and sustainable infrastructures.”
> Simeon Beal, One World Identity.