MOBILE IDENTITY
ENABLING THE DIGITAL WORLD

2020

ABOUT THE GSMA

The GSMA represents the interests of mobile operators worldwide, uniting nearly 800 operators with almost 300 companies in the broader mobile ecosystem, including handset and device makers, software companies, equipment providers and internet companies, as well as organisations in adjacent industry sectors. The GSMA also produces industry-leading events such as Mobile World Congress, Mobile World Congress Shanghai and the Mobile 360 Series conferences.

For more information, please visit the GSMA corporate website at www.gsma.com

Follow the GSMA on Twitter: @GSMA

First edition January 2020

CONTENTS

1 EXECUTIVE SUMMARY

BY RICHARD COCKLE, GLOBAL HEAD OF IDENTITY AT GSMA

DIGITAL IDENTITY SYSTEMS GROWING IN IMPORTANCE

In 2018 the average number of online accounts requiring a password was estimated to be 23 per user, however the average number of passwords was just 13.[1] Some estimates even suggest users re-use passwords as many as five times across different accounts – meaning that with just one data breach, fraudsters could gain access to multiple sites via a single credential.[2] Add to this the 4.5 billion records[3] already exposed worldwide in the first half of 2018, then the threat from identity fraud becomes very real, and just part of the reason why secure digital identity is growing in importance for the digital economy – the challenge will be to balance improved security with an improved user experience.

DIGITAL IDENTITY RELIANT ON MOBILE TECHNOLOGIES, DEVICES AND NETWORKS

'Mobile identity' refers to the mobile technologies, systems, devices and networks used to facilitate digital identity services – services which are often reliant on the ubiquitous coverage of cellular networks that have over 5 billion mobile subscribers worldwide in 2020.[4] Recent analysis from Juniper Research estimates that growth in mobile digital identity solutions could exceed 800% over the next five years, as emerging economies turn to mobile by default. This research also shows that unique mobile identifier services could become the primary source of identification for over 3 billion people by 2024 – providing significant potential for mobile operators to play a primary role in digital identity.[5]

OPERATORS' MOBILE IDENTITY 'TOOLKIT' HELPS THE DIGITAL WORLD GO ROUND

Mobile operators have a unique set of tools and capabilities which provide critical value to the digital identity ecosystem helping the digital world go round. These tools include: know-your-customer (KYC) datasets, which operators are regulated to maintain, that can help with on-boarding and identity verification; or changes in the pairing between subscriber, device and network, that can indicate potential fraud. Tools such as these are collectively referred to in this paper as the 'mobile identity toolkit'. This paper discusses mobile operators' existing tools for mobile identity – and opportunities to develop new ones leveraging big data, artificial intelligence and behavioural biometrics.

MOBILE OPERATORS GAINING SIGNIFICANT TRACTION IN DIGITAL IDENTITY

Worldwide, mobile operators are recognising and commercially deploying their unique digital identity tools and resources. A conservative estimate of mobile operator authentication services puts their monthly active users at close to 1 billion. Mobile Connect, the secure universal log-in solution developed by the GSMA and its members, has now been adopted by 70 operators in 40 countries. Furthermore, operators are entering new markets beyond authentication including fraud detection & prevention and credit scoring with growing numbers of businesses looking to adopt these operator services directly and through operators' channel partners.

OPTIMISING TRUST AND SCALE ARE PRIMARY FACTORS FOR SUCCESS IN DIGITAL IDENTITY

Affirming businesses' trust in their customers and transactions is a primary purpose of digital identity systems. To achieve this subscribers must trust identity services if they are to share their data, and identity services must be trusted by businesses if they are to sell products derived from that data. Trust both ways is critical, but without optimum scale that trust cannot be converted into commercially viable propositions. This paper considers three factors critical for trust, and three critical for scale, which together can yield success in digital identity. For trust we will examine security by design, transparent trust endorsements, and control and privacy for the user. For achieving scale, we will look at interoperability and federation, partnerships and collaboration, and compelling business value.

1 World Password Survey, McAfee, 2018
2 The 2019 State of Password and Authentication Security Behaviors Report, Ponemon Institute 2018
3 Gemalto's Breach Level Index, 2018
4 GSMA Intelligence, 2020
5 Digital Identity: Technology Evolution, Regulatory Analysis & Forecasts, Juniper Research, 2019

2 INTRODUCTION

Digital identity is described by the GSMA, the World Bank, and the Secure Identity Alliance as "a collection of electronically captured and stored identity attributes that uniquely describe a [real] person within a given context and are used for electronic transactions." Having a digital identity proves that we are who we say we are online – but having too many passwords to remember often makes our registration and login experience inconvenient, meaning we give up.

Essentially there are two approaches that could make life easier for users. Firstly, a unified or common digital login:[6] a single set of authentication credentials to remember and use as a universal login across multiple websites would go some way in solving the problem. Secondly, if the user had a single verified digital identity with a single set of credentials from the very beginning, entirely under their ownership and control, it could be used to log in directly or to set up a separate common digital login. Convenient and secure digital identity solutions such as these are increasingly important to underpin the digital economy, where they can drive business revenues. Recent estimates from McKinsey Global Institute across seven countries suggest that successful deployment of digital identity could enable incremental economic growth in developing markets – equivalent to as much as 13% of GDP by 2030 – and up to 3% in more developed markets.[7]

With fraud and cybercrime estimated to cost organisations $5.2 trillion[8] globally over the next five years, business demand for trustworthy and qualified customers is growing fast, catalysed by the effects of international policy and regulation on identity systems. The UN's Sustainable Development Goal no. 16.9 ('Legal Identity for All') focuses global initiatives on reducing the estimated 1.1 billion 'unidentified' users to zero by 2030 – and a wave of globally influential new regulation from Europe and elsewhere (including GDPR, eIDAS, PSD2 and AML) is aimed respectively at improving data protection, federating common digital IDs, strengthening customer authentication, and addressing money laundering. Compliance pressures from these stringent new laws are directly driving online business spend on identity services, data management, and cybersecurity systems, with the average cost of KYC and customer due diligence (CDD) compliance for a financial firm rising to $60 million.[9]

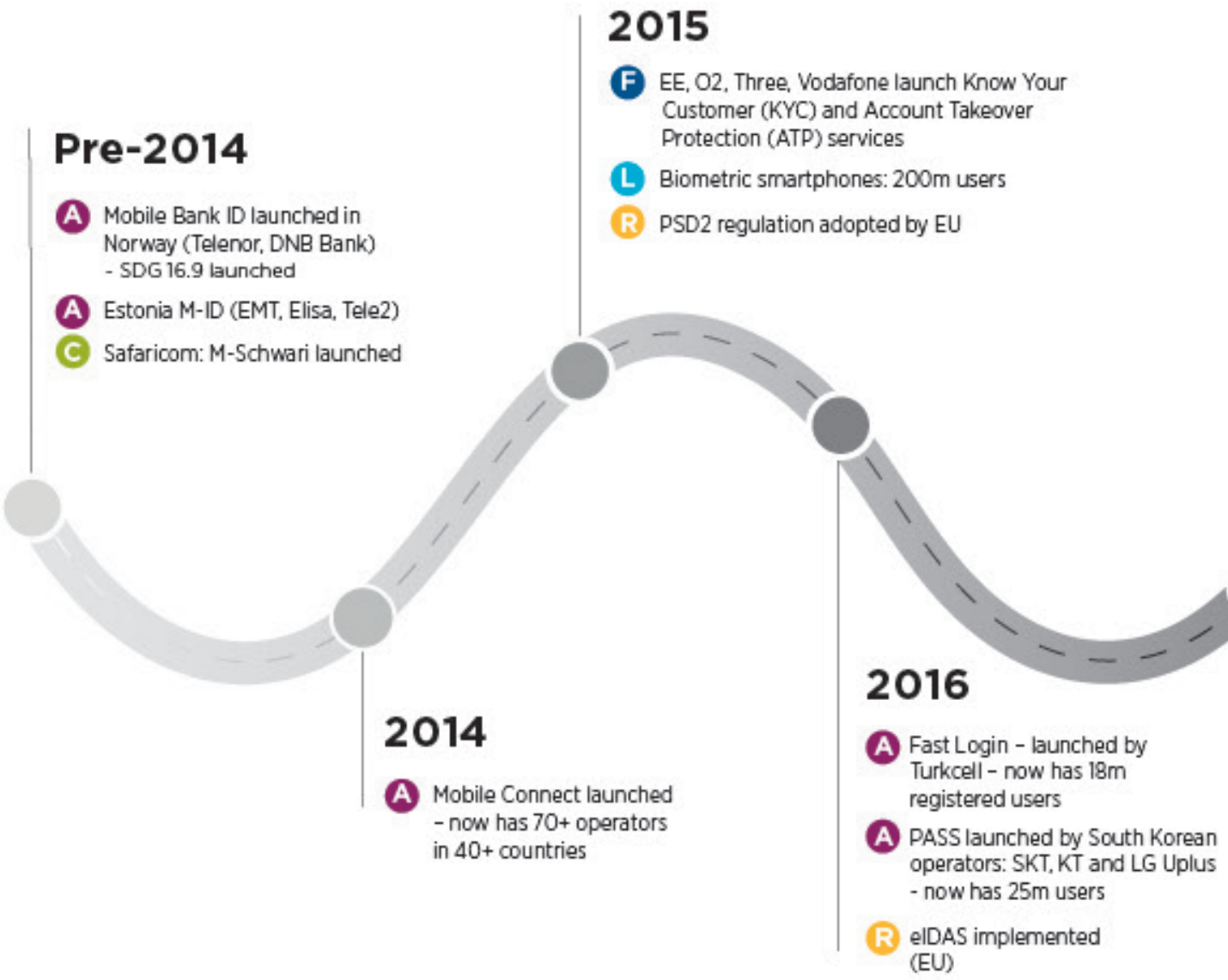
Digital identity systems are becoming a functional pillar of the internet, and mobile identity tools play a growing role in making them more accessible, robust and secure.

6 Common digital identity is used to represent alternative phrases including unified, reusable, universal or Federated Identity
7 Digital Identification: a key to inclusive growth, McKinsey Global Institute, 2019
8 https://www.accenture.com/us-en/insights/security/cost-cybercrime-study
9 Thomson Reuters Know Your Customer Surveys, 2016

3 MOBILE OPERATOR IDENTITY - A TIMELINE

For some years mobile operators have recognised the importance of taking a role in digital identity and have deployed services and solutions in response. Our timeline over the last 5 years illustrates significant landmarks and some key successes that have been achieved by mobile operators by acting on the commercial value of their unique identity assets and resources (figure 1):

FIGURE 1: MOBILE OPERATOR IDENTITY TIMELINE (LAST 5 YEARS)



KEY

A Authentication F Fraud prevention & detection C Credit scoring L Landmark statistics R Regulation

2017

- A itsme - Belgian mobile ID launched by mobile operators: Orange, Proximus, Telenet and Belgian banks
- A 'Mobile Connect et Moi' launched by Orange (powered by AriadNEXT)
- A Indian government ID service, Aadhaar, linked to mobile phone number
- C Czechia X-MNO Credit Risk Score (Vodafone; O2, T-Mobile)
- C MTS Russia: Credit Risk Score

2018

- A Verimi digital ID consortium including T-Mobile launched in Germany
- L Average number of login accounts per user – 23
- R GDPR implemented (EU)
- R AML5 regulation into force

2019

- A China Mobile's authentication service, 'One Quick Login': 700m monthly active users, 117bn daily transactions, 3,300 apps
- A US operators: AT&T, Sprint, T-Mobile & Verizon collaborate to launch ZenKey authentication
- A Telia Identification Broker Service (TIBS) – First deployment in Nordics and Baltics
- A Russian operators: Beeline, MegaFon, MTS and Tele2 roll out Mobile Connect
- L Swiss Mobile ID (Salt Mobile, Sunrise, Swisscom) roll out two factor authentication
- L Fraud Detection & Prevention estimated total market value - $24bn
- L MSISDN-based authentication – MAU – 0.9 bn

Source: GSMA Intelligence

Mobile operators, particularly those with a significant programme of value added services have initiated their identity journey by launching single-sign-on (SSO) authentication to enable convenient and qualified access to these services as well as to their customer care portals, with the purpose of driving their usage and reducing cost in managing dozens of access points; for instance, this is why Turkcell launched 'Fast Login' in 2016, an authentication solution that now has 23 million registered users.

But initiating authentication for their own services has just been the start for operators, it wasn't long before online businesses recognised that adopting operator authentication could attract operator subscribers with easy login as well; for instance by 2016 PASS, the authentication solution developed by SKT and leading South Korean operators, had been opened up to third parties now numbering as many as 32,000 partner companies.

E-commerce is a global marketplace where national borders can become barriers to expansion unless a solution can be found to ease cross border transactions. Something that was appreciated by the mobile industry 5 years ago leading to the genesis of Mobile Connect, developed by the GSMA and its members, to federate operator authentication solutions to do just that. Launched in 2014, Mobile Connect has now been deployed by 70 operators across 40 countries.

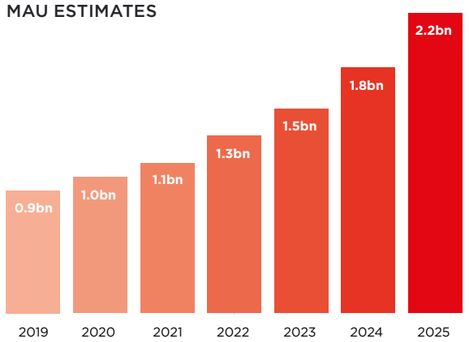
However, other operators started their identity journey from a different place, preferring to target legitimate or consented data services to help businesses trust and qualify their customers, comply with regulation, and fight fraud. UK operators (O2; Vodafone UK, Three UK and EE) for example launched Account Takeover Protection (ATP) services in 2015 to provide businesses with signals for detection and prevention of fraud.

Mobile operators are realising the digital identity opportunity by matching their unique assets with the growing demand for identity solutions: Mobile-ID is a secure digital ID in Estonia from EMT, Elisa and Tele-2 for accessing e-services and digitally signing documents with over 200,000 users; Swiss Mobile ID login and signature solution launched by Swisscom in 2013 has now been adopted by all operators there, and has 3 million SIM cards in circulation.

Now dozens of mobile operators are developing their mobile identity 'toolkits' to create new identity products, services and capabilities that are helping to enable the digital economy. More announcements in 2019 have seen leading US operators (AT&T; Sprint; T-Mobile and Verizon), launch 'ZenKey', a common digital login; and Russian operators (Beeline, MegaFon, MTS and Tele2) launch Mobile Connect, the industry's federated digital identity solution, to third party service providers.

The last 5 years have shown mobile operators achieve measurable traction in the digital identity field. In 2019, it is estimated the industry has reached nearly 1 billion Monthly Active Users (MAU) of MSISDN-based authentication services alone, with conservative estimates putting that figure at 2.2 billion by 2025, a growth rate of 17% CAGR (see figure 2).

FIGURE 2: MOBILE OPERATOR MSISDN-BASED AUTHENTICATION MAU ESTIMATES

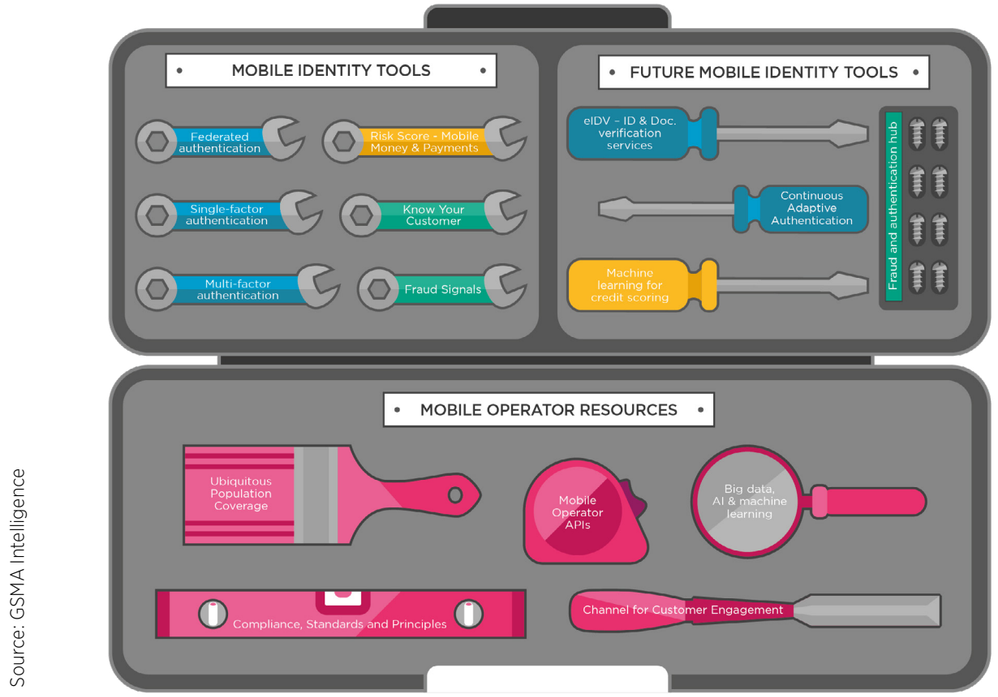


Source: GSMA Intelligence

4 MOBILE OPERATORS' EVOLVING IDENTITY CAPABILITIES AND SERVICES

Mobile operators are making considerable progress in the field of digital identity by unlocking their under-utilised but valuable mobile identity assets and resources referred to here as 'mobile identity tools'. The mobile identity toolkit contains databases, services and resources based on mobile technologies, devices, networks and BSS/OSS systems. It contains existing tools that many operators already offer to the digital identity ecosystem and potential 'future' tools for operators to develop. An indicative range of mobile operators' digital identity tools is illustrated in figure 3 and explained in the following section:

FIGURE 3: OPERATORS' MOBILE IDENTITY TOOLKIT



Source: GSMA Intelligence

4.1 MOBILE IDENTITY TOOLS FOR IDENTITY VERIFICATION AND AUTHENTICATION

OPERATOR SINGLE FACTOR AUTHENTICATION

Many operators have rolled out their own SSO authentication for convenient access across their own value-added services, normally using SMS OTP, USSD or header enrichment authenticating technologies. The mobile operator does this by verifying that the user accessing the business is in control of the MSISDN associated with the account holder. Authentication mechanisms can also be used when required to gain authorisation or consent from users for the sharing of their data.

OPERATOR MULTI-FACTOR AUTHENTICATION

Multi-factor authentication uses two or more factors, and sometimes SIM applet authenticating technology to create a simple user experience. This means a PIN is used as the second factor, which is stored on the SIM card and never transmitted. The authenticating technologies' interactions and messages happen over an encrypted channel, making man-in-the-middle (MiTM) attacks more difficult during authentication.

FEDERATED AUTHENTICATION

Mobile identity federation platforms such as GSMA's Mobile Connect or Telia's Identification Broker Service (TIBS) can federate operators' authentication services making them inter-operable across participating service providers effectively creating a common unified login. Operators' ability to drive scale for their authentication services is boosted when they are designed to be internationally federated, essential for the national and cross-border coverage required to attract major third-party service providers.

FUTURE TOOL: CONTINUOUS ADAPTIVE AUTHENTICATION

In the last few years AI is being applied in a new approach called the continuous adaptive risk & trust approach (CARTA[10]). This approach considers both trust and risk as dynamic properties best assessed and responded to on a continuous contextual basis. Future mobile identity tools could utilise continuous adaptive authentication as an 'invisible' authentication service that reduces user friction and allows businesses to adopt a contextual approach to security. Continuous adaptive authentication works continually or frequently in the background using behavioural biometrics or other data sources to re-authenticate users multiple times depending on the level of risk reflected in contextual or behavioural signals. Abnormal behavioural patterns could trigger step-up authentication to a higher assurance or even reverification of identity (e.g. by face ID). The financial services and technology industries are finding AI and advanced analytics technologies are providing significant value in combatting fraud, according to a PwC survey, 40% of businesses are claiming value from alternative strategies such as 'continuous monitoring'.[11]

10 CARTA – Continuous Adaptive Risk & Trust Approach (Gartner)
11 Global Economic Crime and Fraud Survey, PwC, 2018

FUTURE TOOL: eIDV- IDENTITY AND DOCUMENT VERIFICATION SERVICES

Electronic identity verification (eIDV) verifies a person is who they claim to be by attempting to match information gathered at registration or login with a range of public and private databases including mobile operator information, credit bureau data, social security, police, and vehicle history data. Personal ID documents including driver's licenses, passports, birth certificates, social security cards and citizenship certificates can be used for verification when combined with digital proofing techniques. These proofing techniques utilise AI and machine learning to confirm the co-presence of a 'liveness-proved[12]' face shot or video with their ID document, then authenticate the document, and if necessary add knowledge-based user attributes, and wallet-based factors to verify a person's identity. Mobile operators are well placed to offer a service like this and enhance it with additional security factors that come from their ability to pair device, phone number and subscriber.

4.2 MOBILE IDENTITY TOOLS FOR FRAUD DETECTION AND PREVENTION

KYC DATA

Mobile operators are one of the key industries regulated by many governments to 'know their customers'. With the appropriate legal basis, which can include user consent, operators are in a position to provide KYC data to identity services that corroborates or improves accuracy of those services' own customer records potentially with real-time availability.

FRAUD SIGNALS

Mobile operators can monitor the pairing between subscriber (IMSI), phone number (MSISDN) and device (IMEI) identifiers, any change being an indicator of a potential 'account takeover' (ATO) fraud. Combinations of dynamic network data such as call forwarding and SIM swap information can provide important fraud signals in real time.

FUTURE TOOL: FRAUD AND AUTHENTICATION HUB

Operators are already working to integrate legacy data silos across cybersecurity, network management, customer service, service assurance and separate vendor partners. Holistic consideration of big data from an engineering and data science perspective and the application of AI and machine learning to it could bring the power of 'optimised combinations' to the mobile identity toolkit; that is the massive potential coming from so many different combinations of under-utilised and diverse data sets will strengthen operator's identity products and services opening up new revenue opportunities. The combination of anti-fraud and authentication, two closely related processes, through a single API could provide greater simplicity, flexibility and cost efficiency for businesses combatting fraud. Fraud and authentication hubs that orchestrate multiple identity services into a decision engine are expected to gain ground, with mobile operators having considerable potential to take on such a role.

12 Liveness - proving image is of a real live human face without disguise

4.3 MOBILE IDENTITY TOOLS FOR FINANCIAL IDENTITY AND CREDIT SCORING

MOBILE MONEY & PAYMENT RISK SCORE

Last year's GSMA report on the mobile money industry found 272 mobile money services, and 866 million registered mobile money accounts live in 90 countries.[13] With $1.3 billion transacted every day, mobile money accounts can provide credible financial data for use in developing alternative credit scoring systems, something already being explored by mobile operators and their partners.

FUTURE TOOL: MACHINE LEARNING FOR CREDIT SCORING

'Financial identity'[14] and existing credit scoring products from operators can be based on subscriber information that comes from; KYC data, mobile money transactions, prepaid airtime top ups and loans, device financing, card payments, risk management services and operators' own paid for VAS. Machine learning, however, is expected to unlock new ways of generating alternative credit scores when applied appropriately. 'Branch'[15], for instance, is a start-up that generates alternative credit scores based entirely on smartphone data, which are claimed to be regardless of credit history. Mobile data that is fed, with user permission, into Branch's ML algorithm includes handset details, SMS texts, GPS data, contact lists and billing and repayment history. Mobile operators could do the same by applying specialist vendor ML analytics software residing on their servers, to alternative data and traditional credit histories from billing and mobile money use, in order to roll out new services.

13 State of the Industry Report on Mobile Money, GSMA, 2018
14 Financial Identity as a Service (FiDAAS). Juvo, 2019
15 https://branch.co/

4.4 MOBILE OPERATOR IDENTITY RESOURCES

INTRODUCTION

Certain mobile operator resources and capabilities are included in the mobile identity toolkit as they are often uniquely and fundamentally supportive of the development and delivery of mobile operators' identity tools. This list may not be exhaustive but reflects the capabilities that operators can bring to the digital identity ecosystem.

UBIQUITOUS POPULATION COVERAGE

By 2025 there will be 5.8 billion unique mobile network subscribers and mobile internet penetration will have reached 86%.[16] Both connectivity and internet penetration drive demand for, and support delivery of, digital identity services, increasingly making mobile identity tools a primary resource for digital identity.

CHANNEL FOR CUSTOMER ENGAGEMENT

Operators control key consumer and business touchpoints, making 'customer engagement' an asset they bring to digital identity. Business and operational support system (BSS/OSS) processes and direct to customer marketing and service provision can be used to both collate identity data and deliver identity systems. Already governments in at least 147 countries (as of January 2018) make it mandatory for mobile users to present proof-of-ID when registering for a prepaid SIM card. This enables operators to collect valuable digital credentials, which could be made available for digital identity services with the appropriate legal basis and permission.

COMPLIANCE, STANDARDS AND PRINCIPLES

Mobile operators work to stringent regulations and national laws, and the economic importance of their networks engages them regularly with government policymakers. The mobile industry also leverages global standards to develop a consistent and standardised set of services for managing digital identity. Adding to this the privacy principles associated with operator identity services, puts mobile at the heart of the digital identity ecosystem. The local government and institutional relationships that operators work to maintain often encourage the public sector to involve them in national digital identity initiatives through public private partnerships, as seen in Finland with the launch of 'Mobiilivarmenne'.

BIG DATA, AI AND MACHINE LEARNING

AI-powered big data analytics has been adopted by mobile operators applying it to multiple layers of their business across networks and services. Virtualisation of the network and the fragmentation of the supply chain has required AI to become a foundational technology for the mobile industry. In future, such powerful AI resources could also be leveraged by operators for the mobile identity toolkit to generate predictive risk management products, and behavioural authentication systems that can be delivered in real-time.

MOBILE OPERATOR API PLATFORMS

In software supporting mobile networks, operator APIs (application programming interfaces) make it possible for third parties to use certain mobile network functions within their applications. API platforms are of growing importance to the mobile industry with overall global telecom API related revenue estimated to reach nearly $320bn by 2023[17] This emphasises operator commitment to increasing the value of their subscriber, network and BSS/OSS systems that they expose to external developers via APIs with the appropriate permissions. If the industry's mobile identity tools are to become more accessible, operator API platforms will be an essential resource.

16 GSMA Intelligence, 2020
17 https://www.researchandmarkets.com/research/rxq3vq/carrier_b2b_data?w=12

5 DIGITAL IDENTITY VERIFICATION AND AUTHENTICATION

5.1 INTRODUCTION

The following chapters explore the application of mobile identity tools to use cases organised into three different identity sectors: 'digital identity verification & authentication', 'fraud detection & prevention' and 'financial identity & credit scoring'.

Identity verification and authentication are not the same thing but both are essential to provide simple, secure and qualified access to online services that require them. Identity verification links a real individual to the validated identity information they provide on enrolment. Authentication, on the other hand, is the matching of the identity presented by the user to that recorded on the system, to a certain level of assurance. This is done using different factors of assurance to prove you are who you say you are. For example secure customer authentication may include two or more of the following factors; 'something you have' (e.g. mobile device), 'something you know' (e.g. password, mother's maiden name etc) 'something you are' (e.g. fingerprint, face, iris) and increasingly something you habitually do (e.g. your mobility, typing style or behavioural profile).

Two forms of authentication are designed to reduce the number of credentials that users need to remember and reduce the time taken to login when accessing multiple service providers. The first, digital single sign-on (SSO), is used by enterprises and uses a single authentication credential for accessing multiple systems within the same organisation. A few examples of digital SSO solutions come from Okta, SecurID, Azure AD. The second, federated or common digital authentication[18] uses a single unified authentication credential for accessing multiple businesses. Examples of common digital ID include Mobile Connect, Facebook Login, Google Sign-In, and Sign-in with Apple. Both approaches are set to spread further as businesses look to improve and secure their customers' user flow.

5.2 MARKET TRENDS AND DRIVERS

USER AUTHENTICATION EXPERIENCE STILL HIGHLY FRICTIONAL

Research by email specialist Dashlane estimates that we could have as many as 200 login accounts each by 2020,[19] but people's ability to remember passwords for even half of those is untenable. Dropped logins where users admit to having given up logging in or registering is already as high as 87%.[20] For e-commerce the situation is not much better with nearly 70% abandoning shopping carts because of registration or payment completion difficulties.[21] Moreover, the average time before a user gives up on an application altogether was found to be 14.3 minutes, but nearly one in three (29%) applications take more than 20 minutes to complete making better automation and security of on-boarding a key use case for digital identity.[22]

DEMAND FOR TRUSTED INSTITUTIONAL SUPERVISION

In the GSMA Intelligence Consumer Survey, the top answers to the question 'what steps could companies take to make you feel more confident about the safety and security of your personal data' suggest that involvement of public institutions or central authorities could still be important for building trust with consumers:

- 44% said 'demonstrate adherence to globally recognised cybersecurity standards';
- 39% said 'face heavy penalties for misuse or negligence in the use of my data'; and
- 33% said 'show an endorsement from a government regulator'.

These answers demonstrate that transparent institutional endorsements still carry weight with consumers when evaluating the trustworthiness of a company or service.

18 Common digital identity is used to represent alternative phrases including unified, reusable, universal or Federated Identity 19 https://blog.dashlane.com/infographic-online-overload-its-worse-than-you-thought/
20 https://www.gsma.com/identity/wp-content/uploads/2015/06/mc_factsheet_web_06_15.pdf
21 https://baymard.com/lists/cart-abandonment-rate
22 Battle to Onboard III, Signicat, 2019

PUBLIC PRIVATE PARTNERSHIPS WITH FEDERAL GOVERNMENTS

Public national eID schemes are often born out of a government's wish for their services to be more easily and frequently accessed, but can fail to gain traction when government services are used infrequently. In the UK only 3% have registered with the government's digital ID scheme,[23] and in Germany only 18% have done so.[24] A problem thought to stem from a lack of data sharing and interoperability with the private sector resulting in a low perceived value with users. Governments are finding the answer to this problem is wider public private partnerships and collaboration with existing digital identity services. Partnering with mobile operators or forming wider consortia, including banks and major national corporations to launch eID, benefits from their existing scale, trusted relationships and technical knowhow. Estonia has demonstrated the success of its public private partnership for 'id-card' where 98% have the card with 67% using it regularly.[25]

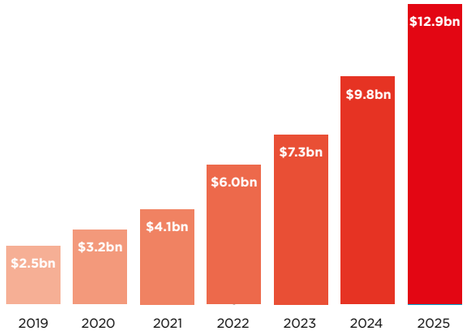
DIGITAL ON-BOARDING SHOWS COST REDUCTIONS

Identity verification and authentication services are expected to grow as businesses recognise that managing their own on-boarding and login can be costly and behind the curve in terms of compliance, development and security. In India, it is estimated the Aadhaar identity system could reduce on-boarding costs of the average firm from $23 to just $0.15.[26] In Norway, it is estimated BankID reduced the time associated with applying for university housing from 10–14 days to 1–3 days.[27] It is thought enterprises requiring high levels of assurance for customer registration could save as much as 90% of costs with times to register reduced from weeks to minutes.[28]

SERVICEABLE MARKET VALUE ESTIMATED TO HIT $2.5 BILLION IN 2019

Serviceable market value for MSISDN-based authentication services is expected to approach $13 billion by 2025 showing growth of over 30% CAGR (see figure 4).

FIGURE 4: MOBILE OPERATOR MSISDN-BASED AUTHENTICATION MARKET VALUE ESTIMATES



Source: GSMA Intelligence

5.3 USE CASES FOR THE MOBILE IDENTITY TOOLKIT

MOBILE IDENTITY TOOL: SINGLE FACTOR AUTHENTICATION

Use case: convenient, simple login operators' single factor authentication enables service providers to offer users a more convenient login experience, by entering their phone number on the company's login page and clicking yes to an instant notification that is returned to their screen. This method makes no request for additional credentials making it a lower level of assurance (LoA2), which can be used as a secondary factor for authentication, when combined with a username and password.

TURKCELL

Turkcell example: Fast Login

As part of a strategy to drive growth of their consumer proposition, Turkcell rolled out an array of apps and services including the TV+ streaming platform, Dergilik magazine media app, and Fizy music platform. It was recognised early on that these new services would benefit from easier SSO authentication for registration and login, leading to the launch of Turkcell's Fast Login solution in 2016. The solution verifies a service user is in control of their mobile phone through a single-factor or two factor authentication process. Fast Login also utilises Mobile Connect, allowing operators to federate their authentications solutions by matching an individual to their phone number and operatorr.[29] Expansion of Fast Login to external businesses followed in 2018 and by the end of 2019, it had more than 23 million registered customers in Turkey – 16 million of these were Turkcell SIM customers and seven million were non-Turkcell mobile users – and was used more than 32 million times across 86 integrated services in that month alone.[30]

中移互联网 China Mobile Internet

China Mobile example: MSISDN Verify "One-click quick login" is China Mobile's common digital identity solution powered by Mobile Connect. Launched in 2017, the solution now has over 650 million monthly active users (as the end of 2019) logging into over 5,000 external service provider apps. The one-click authentication and login scheme refers to the provision of corresponding services for the user by entering the local number or the gateway's automatic authentication number (instead of the username and password) and being verified by the operator's network. Complementing the SMS verification code authentication, the solution can optimize the application login security scheme. This solution relies on the operator's five core resources "number, SIM card, text message, phone call, and Internet access", and combines the Internet business scenario to achieve the upgrade of communication capabilities to IT capabilities. It provides a neutral and open identity system surrounding mobile phone number for Internet services, and facilitates the interconnection and interconnection of services, users and data.[31] [32]

23 https://resources.signicat.com/hubfs/Downloads/the-battle-to-onboard-3-signicat.pdf
24 https://www.signicat.com/resources/federated-electronic-identities-what-are-they-what-are-the-benefits-and-do-they-work
25 https://e-estonia.com/solutions/e-identity/mobile-id/
26 Private Sector Economic Impacts from Identification Systems. Word Bank, 2018
27 Norwegian Mobile BankID: Reaching scale through collaboration, GSMA, 2014
28 Digital Identification: a key to inclusive growth, McKinsey Global Institute, 2019
29 Developed by the GSMA and its member operators- 'Mobile Connect Turbocharges New Services' (April 2019)
30 https://www.gsma.com/identity/wp-content/uploads/2019/05/mc_turkcell_cs_11_04-FINAL.pdf
31 For service providers being accessed over a mobile network only
32 https://mobileconnect.io/wp-content/uploads/2019/02/MC-Verified-MSISDN-functional-datasheet-FINAL.pdf

MOBILE IDENTITY TOOL: MULTI-FACTOR AUTHENTICATION

Use case: Strong secure login
Multi-factor authentication, otherwise termed strong customer authentication (SCA) by the EU's PSD2 regulation, uses two or more factors to authenticate a user at login. The objective is to present a layered defence to fraudsters with multiple barriers if one factor is compromised. Secure multi-factor authentication has wide application (e.g. VPN login, banking login, or gaming accounts), is more secure than existing SMS-OTP solutions and more convenient than legacy authentication methods such as hardware tokens. More recently a consortium-based approach has seen mobile operators partner with national banks and federal government in a public private partnership to achieve the scale, operational resources and levels of trust needed for successful national ID deployments. Mobile operators recognise that mutual cooperation and collaboration in mobile identity helps to drive scale.

itsme example: Mobile identity verification The 'Belgian Mobile ID' consortium was set up to develop a digital identity for users to prove their identity online. The idea was to enable Belgians to conveniently access a whole range of online applications such as banking, government services, insurances, e-health as well as create online accounts, confirm payments and sign official documents (QES). The combined efforts from the consortium's mobile operators (Orange Belgium, Proximus, Telenet) and Belgian banks, resulted in the launch and adoption of the 'itsme' app, a digital ID of level of assurance high recognised by the Belgian government and EU Commission. To use itsme, users have to be over 18 years old with a Belgian eID and a smartphone. itsme only works through the right combination of a user's mobile and its SIM, the itsme app and 5-digit passcode. Service providers adopting itsme are committed to only ask for user data if strictly necessary, which is not shared without the explicit consent of the user. As of the end of April 2020, itsme had 1.7 million registered Belgians with 5 million transactions per month. itsme was launched in Luxembourg in February 2020[34]

SK Telecom example: PASS authentication app
Having separately experienced limited uptake of their authentication solutions, in 2015 SKT, KT and LG Uplus agreed to work together to improve their joint coverage and appeal to businesses. In 2016, the operators federated their separate solutions, now jointly branded PASS, using the PASS cloud platform and relaunched as an app-based solution replacing the old SMS based one. Once registered on the PASS app, a user is only required to enter their PIN or biometric (fingerprint, iris etc) or use a QR code to enable easy and secure access to a number of services under one app that includes mobile payments. PASS reaches over 50 million people and is now used to access over 32,000 external service providers as well as operator services, with SKT alone posting 7 million monthly active users in May 2019.[33]

ZenKey example: Multi-factor identity authentication
ZenKey is a secure multi-factor identity authentication platform provided through the collaboration of leading US carriers: AT&T, Sprint, T-Mobile and Verizon. With a potential reach that covers most of the US population, ZenKey can enable users to log into participating third party apps and websites securely and easily without the need for passwords. ZenKey applies encryption technologies to a user's phone and mobile network when a user logs in either through their smartphone, personal computer or other smart device. Multi-factor authentication is carried out using unique mobile identity data during authentication including phone number, phone account type, user credentials, account tenure and SIM card details.[35]

MOBILE IDENTITY TOOL: FEDERATED AUTHENTICATION

Use case: Convenient and secure cross-border authentication
In the global digital economy users and businesses need to transact across country borders, but if authentication systems are not interoperable users still have to maintain too many sets of credentials to do this conveniently. However, a federated login lets subscribers use the same credentials to access any service provider that is participating in the federated login platform:

Mobile operators already address the identity verification and authentication market through a range of authentication products but are well placed to take their identity role further by adding new enhanced mobile identity tools for on-boarding and authentication or even by becoming an Identity provider themselves. Operators' strong subscriber and business engagement could enable them to move downstream in the identity ecosystem to offer identity provision.

Future mobile identity tools could include enhanced solutions for behavioural biometrics, document authentication and liveness testing, technologies that are already being explored within the industry.

Telia example: Cross-border authentication service
Telia, the mobile carrier and Ubisecure, the identity specialist, initiated the Telia Identification Broker Service (TIBS), a Nordic and Baltic cross-border authentication platform offering several strong authentication methods under one service agreement and integration. TIBS removes the need to maintain several independent authentication platforms with various identity providers. It supports multiple federated protocols and brokering enabling both compliance and scale across the region. The Finnish Population Register Centre deployed the service in early 2019 enabling Finnish citizen access to national services across tax administration and health records.[36]

33 https://www.gsma.com/identity/wp-content/uploads/2018/10/SKT-Turkey-presentation-final.pdf
34 https://www.itsme.be/
35 https://myzenkey.com/
36 https://www.ubisecure.com/news-events/telia-best-consumer-identity-project-award/

6 FRAUD DETECTION AND PREVENTION

6.1 INTRODUCTION

Fraud detection and prevention systems – designed to spot patterns which represent fraudulent behaviour, ideally in real time – are of fundamental importance to the digital economy. Identity fraud, in particular, is a growing concern for online businesses and users alike. Examples include Account Take Over (ATO) attacks, where a legitimate user's details are stolen to take over their online account and profit from its value; or card not present (CNP) fraud, where the customer is not physically present with the merchant during a fraudulent transaction (often carried out online); or even the creation of a synthetic identity, where a fraudster combines real and fake information to create a synthetic identity used to open fraudulent accounts and make purchases.

6.2 MARKET TRENDS AND DRIVERS

VOLUME OF DATA BREACHES ARE DRIVING ACCOUNT TAKE OVERS

In H1 2019 alone, over 3,800 breaches were reported exposing over 4.1 billion records up 54% on 2018.[37] In the US alone, this has caused ATOs to double recording 680,000 in 2018 compared to the previous year.[38] The growing quantity of stolen user data from breaches, sold on the darknet, can be exploited by 'adversarial' AI, leading to ATOs via credential stuffing attacks,[39] as well as being 'productised' for financial, industrial and geo-political gain. The sheer variety of data available on the darknet and from users' digital 'exhaust' is also driving synthetic identity fraud, where fraudsters create artificial identities that cost US lenders alone $6 billion in 2016.[40]

COMPLIANCE PRESSURES CREATING FRICTION FOR BUSINESS

A roster of anti-fraud regulation is putting heavy Know Your Customer (KYC) compliance pressures on business, on financial services in particular, to the point banks recently warned that 'EU rules could scupper a quarter of online payments'.[41] In Europe this is mainly driven by AMLD4/5 and PSD2 regulation, which are ramping up demand for KYC automation technologies.

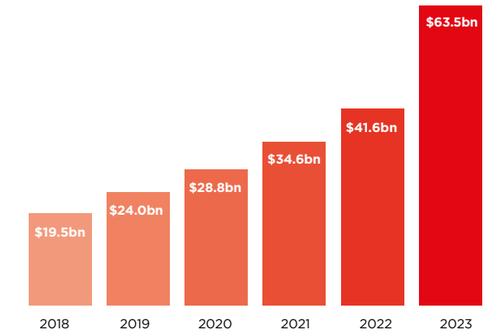
DIGITAL IDENTITY SOLUTIONS CAN REDUCE KYC COSTS BY UP TO 70%

Banks' KYC and Anti Money Laundering (AML) processes alone can cost $2.50 for a basic check and with staff costs added costs rise to between $10 to $150 per check. Digital identity solutions can offer significant improvements to screening processes potentially reducing the cost of KYC and AML processes by up to 70% – and improving the speed of these checks by 80%.[42]

TOTAL AVAILABLE MARKET VALUE NEARS $20 BILLION IN 2019

The total available market value for fraud detection and prevention includes the following services: fraud analytics (big data, predictive and behavioural), authentication (risk based single and multi-factor) and GRC solutions (governance, risk management and compliance). Overall the total available market value for fraud detection and prevention solutions is estimated to be close to $20 billion in 2019 (see figure 5).[43]

FIGURE 5: TOTAL AVAILABLE MARKET VALUE – FRAUD DETECTION AND PREVENTION



Source: MarketsandMarkets/Statista

6.3 USE CASES FOR THE MOBILE IDENTITY TOOLKIT

Financial services including banking, payments and insurance are faced with escalating volumes of transactions and a growing diversity of threat vectors that can be mitigated by operators bringing the following tools to bear:

MOBILE IDENTITY TOOL: FRAUD SIGNALS

Use case: Assuring a new mobile device or password reset

Banks and financial companies, especially, need to protect their customers from ATO attacks. Fortunately, operators can offer insights that indicate when there has been a change that could indicate a fraudulent activity, when for example associating a new mobile device with a bank account. Attributes such as last SIM change, device change, account tenure, or unconditional call diverts that can represent fraud signals are among those that have been found useful for the financial services industry:

37 https://pages.riskbasedsecurity.com/2019-midyear-data-breach-quickview-report
38 US Identity Fraud Study 2019, Javelin Strategy & Research
39 'Credential stuffing' - Automated login attempts using thousands of stolen pairs of credentials e.g. Sentry MBA
40 Synthetic Identity Fraud in the U.S. Payment System, Federal Reserve, 2019
41 Banks warn EU rules will scupper a quarter of online payments, FT, 2019
42 European Digital Lenders: Operating efficiency helping digital lenders attack a $150 billion annual origination market, Autonomous NEXT
43 MarketsandMarkets/Statista

UK operators' example: Phone lost or stolen

In 2015, UK operators O2, Vodafone UK, EE and Three UK defined a set of "Account Takeover Protection" (ATP) services based on the same Mobile Connect/OIDC technical architecture as the KYC Match service. Whereas KYC Match compares only semi-static user information, the ATP service provides dynamic device information as well. Moreover, several signals are available in various bundles serving different security use-cases. For example, mobile operators can provide indications of whether a phone has been reported lost or stolen, the SIM/phone pairing has recently changed, a call divert has been set up on the number, or the number is recycled – all of which could be indicators of an ATO. Using these indicators, a bank, for example, can make a better-informed decision on whether transactions or accounts could be fraudulent.[44]

6.3.2 MOBILE IDENTITY TOOL: KYC 'MATCHING'

Use case: Fraud check matching KYC data and phone number

KYC procedures exist to protect organisations and their customers from fraud and losses resulting from illegal financial transactions.

For this reason operators are regulated to know their customers and have assembled a sizeable registry of user identity data as a result.[45] This data supports KYC matching products that can be applied for use cases such as age verification for legally restricted purchases (e.g. alcohol, restricted content, gambling etc) or changes to bank accounts where a match between user ID and phone number would be carried out to detect fraudulent account changes without impacting the user experience. In 2015 the UK mobile operators launched a KYC match service: Mobile operators already address the fraud opportunity through their fraud signal, KYC and MSISDN tools but could investigate a potential role as a fraud and authentication hub that combines their own growing set of tools with AI-enhanced fraud solutions. Operators could also move downstream in the identity ecosystem to productise their rich data sets and distribute them direct to business.

UK operators' example: Anti-fraud for registration

UK operators O2, Vodafone UK, EE and Three UK have launched a KYC Match product[46] for businesses looking to enhance their registration processes and to meet anti-fraud use cases. It validates a customer's identity by verifying identity attributes paired with the mobile phone number. Standardisation has been an important element to the development of the KYC Match product, and was carried out in accordance with the GSMA's Mobile Connect. Technical cooperation between operators has been a key element in development allowing UK's leading operators to offer businesses near total coverage of UK subscribers.

44 https://mobileconnect.io/wp-content/uploads/2019/02/mc-Mobile-Identification-goes-Live-UK.pdf
45 EU regulations: AML, PSD2
46 the MNO product is an unregulated KYC Match product

TeleSign example: KYC

A partnership between Proximus, Belgium's leading mobile operator, and TeleSign was designed to provide businesses with KYC services to help them comply with the new EU Payment Services Directive, and PSD2. Jeroen Degadt, Director Carrier and Wholesale at Proximus said "Partnering with TeleSign, a global neutral aggregator, was the clear choice. With access to TeleSign's fraud risk product portfolio, we will be able to provide increased security and assurance for our customers across the country." TeleSign believe partnerships like this highlight "the increasing importance of Mobile Identity and the key role played by mobile operators in digital transformation. It represents a new opportunity to mobile operators worldwide to participate in a Global Mobile Identity ecosystem and improve the security of their end users online".[47]

7 FINANCIAL IDENTITY AND CREDIT SCORING

7.1 INTRODUCTION

Lack of access to formal financial services remains a global problem. The World Bank estimates that there are 1.7 billion people excluded from traditional financial services as well as from mobile money services. Fortunately, the banking sector has recognised the aggregate potential of the nearly 4 billion 'low value' customers (68% of adults)[48] mostly in developing countries. Unfortunately, finance companies in many parts of the world are challenged by the lack of appropriate credit history for the world's 1.7 billion unbanked users.[47] In fact, coverage by credit agencies in developing regions such as (sub-Saharan Africa) can be as low as 9%. However, while a user may not have a bank account or credit history they are highly likely to have a mobile phone and mobile payment history. Leveraging over 5 billion subscribers, mobile operators can help the finance industry resolve this problem by providing alternative credit scoring products, consistent with relevant regulation and user permissions, that can also bring them significant new revenue streams.[49] The market for alternative and hybrid solutions for credit scoring and establishing financial identity is expected to grow considerably over the next 3 years.

7.2 MARKET TRENDS AND DRIVERS

OPEN BANKING UNLOCKS ALTERNATIVE CREDIT SCORING

PSD2, the EU's Revised Payment Services Directive has helped to usher in a new era of open banking worldwide. Additionally, the Financial Data Exchange (FDX) was founded to unify the financial industry around a common interoperable standard for secure and efficient transfer of consumer-permissioned financial data.[50] Riding this open banking trend, fintechs are taking on the traditional credit bureaus to provide new techniques for credit scoring.

ALTERNATIVE CREDIT SCORING GROWS HOUSEHOLD CREDIT WORLDWIDE

Digital Identity helps to bring the unbanked into the formal economy – digital transformation of the financial sector, including the extension of alternative credit scoring through mobile operators, could grow household credit worldwide by $408 billion and give 1.7 billion unbanked customers access to financial services.[51] Worldwide, such transformations could also bring 95 million new jobs, and as much as $4.2 trillion in new deposits by 2025.[52]

47 https://www.businesswire.com/news/home/20191022005356/en/TeleSign-Expands-Global-Services-Partnership-Proximus
48 World Bank, Findex, 2018
49 GSMA Intelligence, 2019
50 https://financialdataexchange.org/
51 'The YES Economy: Giving the World Financial Identity' , Juvo/Oxford Economics, October 2019
52 "Digital finance for all: Powering inclusive growth in emerging economies." McKinsey Global Institute, September 2016.

FALSE POSITIVES AN EXPENSIVE PROBLEM FOR THE BANKING INDUSTRY

Online shoppers face three times the risk of mistakenly having their card declined.[53] In the US, Aite Group predicted 30% of card transactions in 2018 were false positives,[50] where legitimate credit-worthy users are falsely declined, an inefficiency in business estimated to have cost US card issuers $331 billion.[54] The mitigation of 'false positives' relies on easily accessible, accurate and queriable identity attribute systems.

7.3 USE CASES FOR THE MOBILE IDENTITY TOOLKIT

Mobile operators' ability to connect unbanked and unidentified populations to the mobile ecosystem and help enable the provision of a financial identity for them is critical if these populations are to effectively engage with e-commerce, government services, regional benefits and global aid. Alternative credit scoring and the maintenance and user control of financial identity are key use cases to which mobile operator identity tools can contribute.

MOBILE IDENTITY TOOL: CREDIT SCORE BASED ON MOBILE OPERATOR DATA

Use case: Creation of alternative credit score

Models built on MNO data are demonstrating an impressive capability and are well regarded by businesses as they add value to their risk assessment strategies. Identity data from mobile money accounts, airtime top-up habits and other account information can be modelled to create an alternative credit score for a subscriber enabling, for example, an airtime loan to initiate a subscriber's credit history.

Mobile operators have the opportunity to move downstream in the credit scoring ecosystem by enhancing and productising their alternative credit data. This can be done by combining more diverse data and applying AI analytics technologies and marketing these services direct to business customers. That said, partnering with specialist channel partners (e.g. Juvo, Branch) is also an option to offer financial Identity services that monetise operator data without the potential investment required to go direct.

53 False Positives: The Undetected Threat to Your Revenue, Vesta Corporation, 2018
54 Aite Group, 2018

M-PESA

M-PESA example:
Alternative credit scoring

One of the first alternative credit scoring operations in Africa was launched in 2012. M-Shwari is a credit and savings product for M-PESA customers launched by Safaricom and the Commercial Bank of Africa (NCBA). To qualify for an M-Shwari loan, a customer must be an M-PESA subscriber for at least 6 months. The alternative credit score is constructed from an algorithm applied to mobile operator data, in this case past use of Safaricom service's M-PESA, Bonga points, voice, and data services. The resulting score determines the initial eligible loan limit with subsequent loan limits based on levels of "regular savings" and loan repayments with M-Shwari. Both loan disbursements and repayments are made through Safaricom's M-PESA mobile money service. In less than a year from launch, the product increased the number of deposit accounts at NCBA from under 35,000 to over 5 million.[55]

Juvo

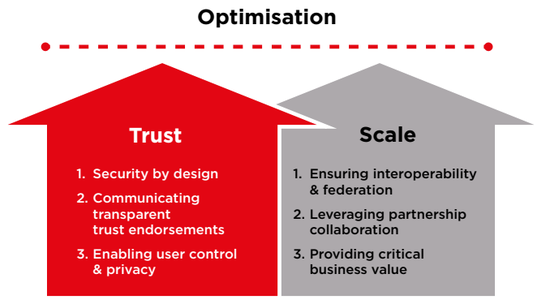
Juvo example:
Financial Identity-as-a-service (FIDaaS)

Mobile network transactions can provide the basis for defining a financial identity for billions of people who have no formal financial history, but do have a mobile phone. A mobile network account top-up is recorded in a centrally-located database, in a digital format and associated with a unique person, which Juvo believes can form the basis of a financial identity and credit score. Mobile operators could use this financial data to provide a low-risk airtime loan to be built on over time potentially leading to partnerships with financial institutions to offer subscribers a wider range of financial services. Additionally, with the right mechanisms for legal consent from end-users there is an opportunity to make financial identity data available to third party service providers to open a new monetisation opportunity for operators.[56]

8 OPTIMISING TRUST AND SCALE FOR DIGITAL IDENTITY

Trust is an important dimension for identity services. Businesses need to trust their consumers and often use identity services to achieve that, while consumers need to trust both the business and identity service to ensure the sharing of their data is legally compliant. Likewise, identity services need to reach optimum scale in coverage, either locally or internationally to attract businesses' interest and in order to become commercially viable. Our analysis has identified six critical success factors for digital identity services arranged into two primary dimensions of trust and scale. These factors can be used as a set of recommendations or check list for mobile operators developing digital identity services (figure 6).

FIGURE 6: OPTIMISING TRUST AND SCALE IS CRITICAL FOR SUCCESS IN IDENTITY MARKETS



8.1 STRATEGIES FOR DEVELOPING TRUSTED IDENTITY SERVICES

SECURITY BY DESIGN

Security is a major pillar of trust, and in a world of growing cybercrime and new technologies used as much by fraudsters as the good guys, protecting the user's data and digital rights will require ever more skill and effort. Security by design is a software engineering approach that is increasingly becoming mainstream for the security and privacy of software systems. But where mobile operators' legacy systems have not yet benefited from the security by design approach the implementation rate of mitigation measures may need to be raised to protect the security of their identity-enabling toolkit.

How can the mobile identity toolkit help?

Multi-factor authentication incorporates additional factors (e.g. biometrics, pin number) of assurance to increase the level of security. For example, China Mobile's SIM Shield is a two-factor authentication tool which secures online remittance and money transfers using the SIM and replaces the need for a token device.

55 https://www.gsma.com/mobilefordevelopment/country/kenya/m-shwari-mobile-money-savings-loans/
56 https://juvo.com/fidaas/

COMMUNICATING TRANSPARENT TRUST ENDORSEMENTS

Identity systems and their business customers must be transparent about their privacy policy and regulatory compliance. An identity system needs a trust framework, a legally enforceable set of specifications, rules and agreements that regulate it. Both online businesses and identity systems should clearly communicate their accreditations, standards affiliations and institutional relationships as all of these are relevant to the consumer's perception of trust.

How can the mobile identity toolkit help? **–** Mobile operators, like many identity solution providers, develop their services to a consistent set of standards and privacy principles under strict regulations covering a number of legal domains to provide a foundation of trust for both user and business.

ENABLING USER-CONTROL AND PRIVACY

The World Economic Forum's (WEF) key security principle for a strong identity system says 'The system should prevent user information from being overexposed, lost or stolen'. While institutions have developed privacy principles and worked on providing more information to users about their privacy rights, mainstream users' interest in them and their ability and willingness to actively manage their privacy themselves appears to be unproven. A recent survey from GSMA Intelligence showed 72% failing to enable a second layer of security and 69% failing to change their privacy settings even after a user was involved in a data breach.[57]

This could be because most users are not aware of the risks or don't care about them, but it could also be because they don't have easy access to the privacy tools and controls that can protect them or just don't trust them.

But as users find themselves increasingly trapped between the over exposure of their data to big tech, and the loss of their data through weak security, then their demand for secure and easy to use privacy and data sharing controls will grow. Some operators are addressing the lack of privacy tools: for instance, Verizon recently launched OneSearch – a privacy-focused search engine. Its default dark mode activates advanced privacy, with search-term encryption that does not rely on cookie tracking, profiling, data storing or personalisation. Search will not be based on consumer habits, but on a wider, deeper range of results, enhancing privacy and reducing bias.

How can the mobile identity toolkit help? – Operators apply 'Compliance, Standards and Principles' to underpin the privacy policies of their identity services. At Mobile World Congress Los Angeles 2019, Johannes Jaskolski of newly launched ZenKey made it clear that with this new service "the user is always in control – this is paramount. Nothing happens unless you set it up. You can be sure that service providers are who they say they are, and once you're comfortable with that, you can choose which data you share with them, with explicit consent every step of the way".

8.2 STRATEGIES FOR SCALING DIGITAL IDENTITY SERVICES

ENSURING INTEROPERABILITY AND FEDERATION

It is unlikely one solution will solve the world's digital identity crisis, therefore making the federation of multiple authentication solutions an increasingly plausible option. A key principle for digital identity outlined by the World Bank's ID4D is to 'create a platform that is interoperable and responsive to the needs of various users'.[58]

Interoperability reduces the fragmentation of supply and reduces user friction improving an identity system's traction, which can be extended by federating identity systems at an international level.

How can the mobile identity toolkit help? – Federated authentication coordinates multiple operators' authentication services making them inter-operable across participating service providers in different countries. Examples include Mobile Connect led by GSMA and its members, and Telia's Identification Broker Service (TIBS).

57 Consumer Survey: privacy concerns, GSMA Intelligence, 2019

58 https://id4d.worldbank.org/principles

LEVERAGING PARTNERSHIPS AND COLLABORATION

As governments the world over see the benefits of making national eID a pillar of their modernisation programmes, they often look to leverage mobile operators' retail presence and widespread agent networks to support enrolment for their new digital identity systems. Public Private Partnerships between government and operator as well as consortium-led models of identity provision can establish clear institutional mandates and consensus on technical standards while ensuring early-stage industry participation that establishes scale from the very beginning. Experience has shown government initiated eID can only scale if it provides value to private sector organisations as well, whose adoption attracts growing numbers of users.

Furthermore, operators already engage with channel partners to provide near term distribution and monetisation for their mobile identity products and datasets. A few examples of channel partners might include TeleSign, Experian, Juvo and Signicat, Idemia and CallSign leading aggregators and providers of identity solutions that utilise global telecommunications data. For operators, optimising scale of mobile identity services will likely require a mix of indirect channel partners such as these and direct services to business depending on the shape of the local identity ecosystem.

How can the mobile identity toolkit help? **–** The regulatory compliance and standards-based characteristics of mobile operators underpins efficient working relationships needed for public private partnerships. Examples include Estonia's M-ID[59] and Germany's European Identity scheme called Verimi.[60]

PROVIDING COMPELLING BUSINESS VALUE

Common digital ID systems exist in a two-sided market (e.g. businesses on one side and users on the other) making scale critical for their success. If there is significant business value in an ID system, its widespread and transparent adoption by online businesses gets noticed by consumers who start to use the common digital ID as well, potentially resulting in the network effects[61] that drive scale.[62] As recognised by the WEF such broad support for identity systems comes from delivering value[63] to all stakeholders making a system commercially viable.[64] For many identity systems delivering significant value to business means offering advanced data-sharing functionality or 'queriability' that enables businesses to access valuable risk management services. Absence of such functionality can lead to low adoption of the system by businesses and failure to trigger network effects.

How can the mobile identity toolkit help? – For instance, single factor authentication (utilising a verified MSISDN) goes beyond authentication and can also provide a background anti-fraud check to quickly identify the status of the number; lost or stolen or spot a recycled number requiring additional checks.

59 https://e-estonia.com/solutions/e-identity/mobile-id
60 https://verimi.de/en - One Account for Everything
61 A network effect represents the increase in the value of a service resulting from an increase in the number of other parties using it
62 https://www.signicat.com/resources/federated-electronic-identities-what-are-they-what-are-the-benefits-and-do-they-work
63 Enhanced value for businesses in: compliance support, security, anti-fraud, customer information and customer user experience
64 A Blue Print for Digital Identity, WEF, 2016

9 CLOSING REMARKS

Mobile operators' entry into the digital identity ecosystem has been carefully considered, and now more operators are offering authentication services and other mobile identity tools that are gaining traction in the market. Monthly active users of operators' MSISDN-based authentication services alone are approaching 1 billion and are estimated to be growing at over 17% a year.[65] Furthermore, several dozen innovative mobile operators are developing their mobile identity services, building on new investment and capabilities in big data, AI, machine learning and APIs to bring more advanced mobile identity products to market.

Identity opportunities available to the mobile industry are expected to grow, with online businesses and channel partners continuing to knock on operators' doors for their unique identity data services. But as cybercrime continues to grow, and regulation tightens, the digital economy is in urgent need of mobile operators' identity services in the near term. Operators should not, therefore, wait to unlock the powerful potential of their unique and under-utilised identity data assets and should start working to combine them with their emerging understanding and capabilities in AI and machine learning.

The GSMA aims to encourage, support and drive operators' involvement in digital identity. In 2020 the association will aim to bring identity players together, so they can share expertise and forge new working relationships.

Partnering for innovation on this increasingly expert footing will give operators already active in identity the opportunity to engage with the developer community, and establish early partnerships with some of the most innovative start-ups in their markets. And for those operators not currently active in the space, exposure to the expertise of those who are can help them to understand and navigate the issues to determine whether entering the identity market is right for their businesses, where the revenue opportunities are, and who they might seek to work with.

For further discussion with GSMA representatives please contact:

- **identity@gsma.com**

AUTHORS:
Richard Cockle, Global Head of Identity, GSMA
Mark Little, Senior Manager, GSMA Intelligence

65 GSMA Intelligence, 2019

GSMA HEAD OFFICE
Floor 2
The Walbrook
Building25 Walbrook
London EC4N 8AF
United Kingdom
Tel: +44 (0)20 7356 0600
Fax: +44 (0)20 7356 0601