THE PAYPERS

Web Fraud Prevention, Identity Verification & Authentication Guide 2018-2019

LATEST INSIGHTS INTO DIGITAL ONBOARDING AND FRAUD MITIGATION FOR BANKS, MERCHANTS AND PSPS

Key Media Partners

mpe Merchant Payments Ecosystem

Endorsement Partners

MRC Building Better Commerce Fraud & Payments Professionals

HOLLAND FINTECH

Web Fraud Prevention, Identity Verification & Authentication Guide 2018-2019

LATEST INSIGHTS INTO DIGITAL ONBOARDING AND FRAUD MITIGATION FOR BANKS, MERCHANTS AND PSPS

Contact us

For inquiries on editorial opportunities please contact:

Email: **editor@thepaypers.com**

To subscribe to our newsletters, click **here**

For general advertising information, contact:

Mihaela Mihaila

Email: **mihaela@thepaypers.com**

RELEASE VERSION 1.0
DECEMBER 2018

TEL: +31 20 893 4315
FAX: +31 20 658 0671
MAIL: EDITOR@THEPAYPERS.COM

Editor’s letter

Customer experience and the **conflict between offering a frictionless customer service to good clients while managing risk and blocking the bad guys** are some themes that are emerging from acquirers, card schemes, regulators, service providers, merchants, as well as auditors and journalists alike.

Identifying fraudulent behaviour without rejecting or offending good customers is key because a blocked good customer will not return, and as the market is so competitive, they can go everywhere. Moreover, *automation technologies based on machine learning and artificial intelligence are gaining prominence* in this conversation. But, as always, some challenges in addressing these themes, security-wise, still remain.

The Web Fraud Prevention, Identity Verification & Authentication Guide 2018-2019

To respond to some of these challenges, **we have released our 7th edition of the Web Fraud Prevention, Identity Verification & Authentication Guide** to provide payment and fraud and risk management professionals with a series of insightful perspectives from industry associations and leading market players on key aspects of the global digital identity, transactional and web fraud detection space.

The guide is structured in three parts; the first part focuses on presenting the industry, with its most acute problems, but also shares some best practices from industry leading players on how to tackle them. With the advent of digitalisation and the use of smartphones, **business and fraud coexist globally, both seen as profitable activities**, involving large masses of customers. The surge in demand for many goods and services has enabled **not only businesses’ profits to soar but also fraudsters to capitalize on this growth**. Bad actors are tricking retailers/merchants/banks by hiding beneath large transaction volumes and exploiting the fact that many products and services providers are willing to accept a greater degree of risk in order to approve more orders.

Key challenges for businesses

One of the biggest **challenges in the fraud detection space** for retailers/merchants is that **for consumers, a transaction needs to happen in the blink of an eye**, and therefore fraud controls should be invisible for them.

However, **fraud attacks are becoming more sophisticated**, with fraudsters having access to the latest technology and sophisticated tools. Therefore, **what is really needed? A fraud management solution can track the customer’s behavioural patterns** (behavioural profiling) and **instantly detect and report any signs of fraud, triggering a step up authentication to mitigate the potential risk** (risk-based authentication).

Similarly, **when it comes to financial institutions (FIs)**, FIs are under intense competitive pressure to **make the banking experience easier and frictionless** (while regulators in Europe appear to be taking the industry in a different direction, thanks to the second Payment Services Directive’s requirement for Strong Customer Authentication).

The faceless nature of the online and mobile channels makes authentication hard, however the large amounts of data that have been breached in recent years combined with fraudsters’ use of phishing, social engineering, and malware make authentication much more difficult. As a result, **some of the top threats for 2018 in ecommerce and banking are account takeover and new account applications, according to Aite**.

For Europe especially, but also for the US, Canada and Australia, in 2018, financial discussions revolved around **Open Banking initiatives**. The concept of open banking **promises users greater control over their financial data**; however, it is not without risks, and **its success is tied to consumer confidence when it comes to the security and privacy of their information**.

At the moment, **businesses have become incredibly dependent on a network of systems to manage, store, and transmit information** such as financial accounts, personally identifiable information, intellectual property, transaction records etc. Within this web, authentication, validation and verification have turned out to be central to the ability of these businesses to effectively secure access to consumer-facing digital channels and the systems that underpin their operations. →

The right tools for fighting fraud

The second part of our **Web Fraud Prevention, Identity Verification & Authentication Guide 2018-2019** focuses on mapping the key players in the **fraud detection, identity verification and online authentication space**. The chapter aims to create an accurate picture of **what the fraud detection, identity verification and online authentication offerings looks like**, and it **displays the key players of the industry together with their main capabilities**. Depicting the most important features of each company is part of our goal of helping merchants, banks, fintechs and payment service providers to grasp the current market opportunities and to use them according to their own needs.

The whole range of capabilities is designed to address the pain points that organizations in the payments space are struggling to remove. To do so, **security and risk management leaders** involved in online fraud detection **have started using machine-learning analytics, cloud-based deployment options, artificial intelligence, behavioural analytics, and massive global data networks**.

Such technologies generate real-time insights into the nuanced patterns of fraud to enable businesses to spot and fight fraud. These patterns are based on geography, industry, time of day, time of year, and over 15,000 other signals. Fraud management specialists/vendors have developed networks that analyse millions of transactions in real time across billions of devices.

Finally, the third part of our **Web Fraud Prevention** guide, the **Company Profiles section**, offers insights into the capabilities fraud prevention companies offer businesses in order to spot fraudulent attacks, stop them and prevent them from happening.

Obviously, we would like to **express our appreciation** to the **Merchant Risk Council** and **Holland FinTech** – our endorsement partners who have constantly supported us – and also to **our thought leaders, participating organisations** and **top industry players that contributed to this edition**, enriching it with valuable insights and, thus, joining us in our constant endeavour to depict an insightful picture of the industry.

To view the report in its entirety, please click here.

Conclusion

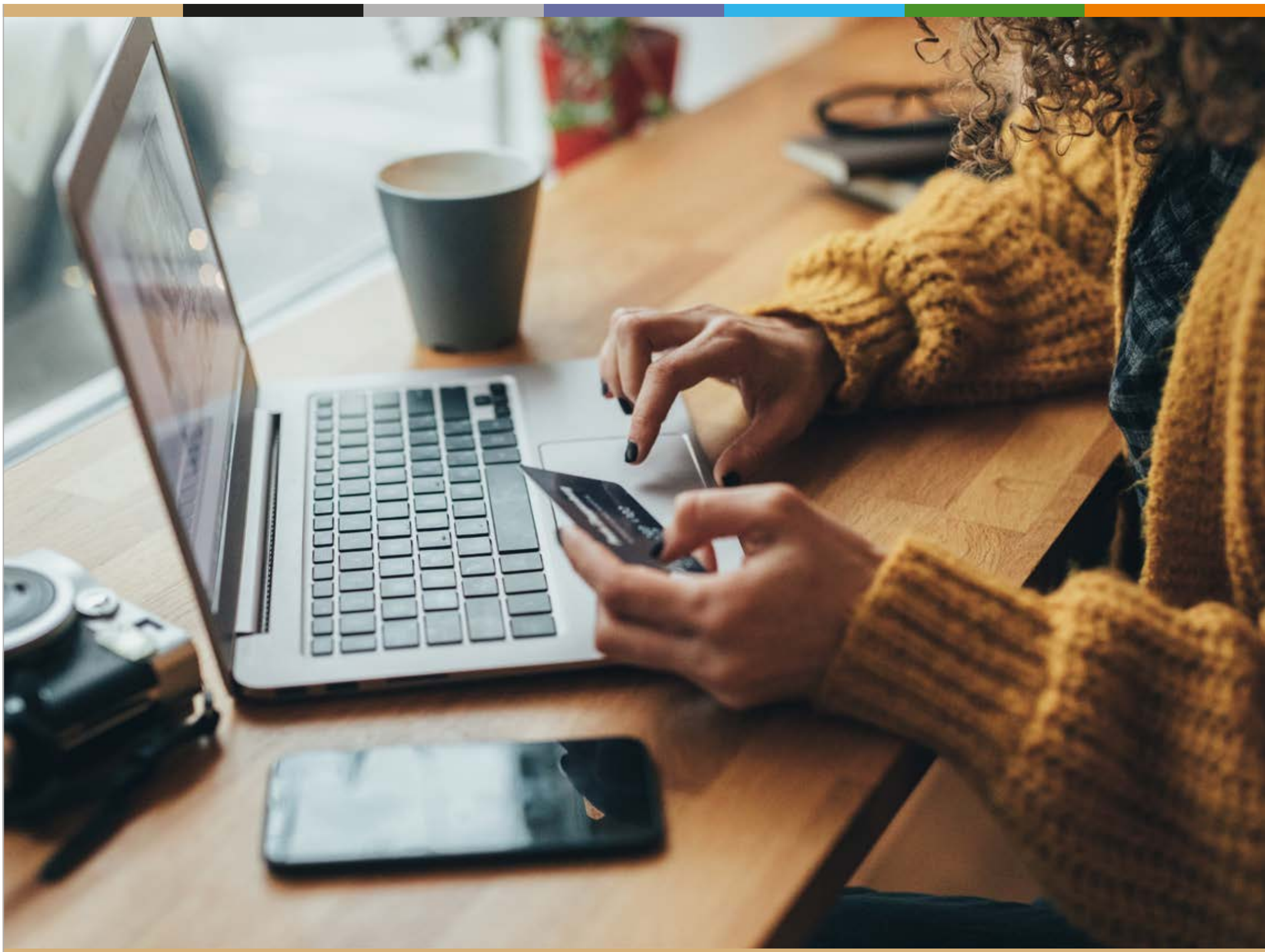
Businesses may think they understand fraud, but the reality is far more complex, and this lack of insight **could lead to guessing, incorrect conclusions, and bad decisions. Premises** such as the **fraudsters as geeky guys, conducting their activities at night in their basements**, and **living somewhere in Eastern Europe**, or that **ATOs are relatively low profile events** could shape businesses' fraud-fighting operations from top to bottom. Moreover, these assumptions help determine how analysts set up rules, how many people the fraud team hires and staffs on a given day, and so on.

Therefore, **security and risk management leaders responsible for fraud prevention and payment security should align with cross-organisational groups** (security, identity and access management, credit/underwriting) to **detect high-risk or anomalous activity** and identity, and **tap into technologies that enable fighting against these threats**. And if we consider the large amounts of harvested data, **the capability of analysing and connecting data across channels is vital for strong defence**.

Enjoy your reading!

Mirela Ciobanu

Senior Editor, The Paypers



Customer Onboarding and Identity Verification

An Introduction to Customer Onboarding and Digital Identity Verification

Mirela Ciobanu | *Senior Editor* | The Paypers

Did you know that 59**% of customers looking to open a bank account have walked away from online applications in the last 12 months**? The reason behind this: many application processes aren't really designed for the digital age.

However, the good news is that **smart fintech businesses** and **challenger banks** are getting under the skin of digital identity and using our uniqueness to unlock a frictionless future. They do so **by tapping into technology** such as **behavioural biometrics, machine learning** and **artificial intelligence**, and lately also blockchain to support secure, intuitive and personalised digital experiences that are beneficial for both companies and consumers alike.

In this chapter, we will see **how the onboarding process looks like**, not only from a **customer's perspective** working with a financial services institution (FI) or other regulated entities, but also from a **FI's perspective onboarding new clients**. Banks are looking for ways to increase conversion of new customers applying for their product/service, be relevant for them, while also **managing risks associated with KYC**/onboarding processes. But customers are demanding **a flexible (mobile first) and modular onboarding process**, and regulators are constantly watching the market and updated/adopt new regulations (e.g. AMLD5).

Will banks be able to get this puzzle right, in time? After all, improving the customer onboarding experience should be a priority for financial institutions, especially since regulations such as PSD2 will enable customers to change their financial service provider more easily.

Onboarding new customers in a digital world: a bank's perspective

After a few years of battles between incumbent banks and smart fintechs/challengers, everyone has agreed that **digital customers need digital processes**. Nowadays, for many financial services organisations, the onboarding process is considered costly, prone to fraud and creates unnecessary friction in the customer's experience. This old approach is simply not sustainable as it gives rise to high abandon rates and does not meet the expectations of a younger digitally 'native' customer.

How is my current onboarding process performing? The incumbents

Because many application processes aren't really designed for the digital age, incumbent banks just replicate traditional onboarding processes, pushing only some parts of it online. As a result, **up to half of digital applicants can't actually complete an application online**; instead, they have to go into a branch to verify their identities, or submit additional documentation. ➔

An Introduction to Customer Onboarding and Digital Identity Verification

In 2016, Signicat conducted a research called the Battle to On-board that aimed to portray the onboarding processes for the UK financial services consumers. The research found that **40% of consumers had abandoned bank applications**; more than 1 in 3 (39%) abandonments were due to the length of time taken and a third (34%) were due to **demanding too much personal information**. Interestingly, the company performed the same research two years later and the results **were similarly devastating for banks**. In fact, it was worse than ever in the UK, with 56% of respondents having abandoned an application. Among other impediments for applying cited by consumers were the fact that they **had to provide personal information by post or take it into the branch**, and sometimes **the language used by the bank was confusing**.

Nevertheless, some progress has been made with banks such as China Merchant Bank, one of the largest credit card companies in China, Wells Fargo and the Bank of America that have **reached out to AI assistants to improve customer experience**. For instance, **Bank of America's 'Erica' chatbot** was designed to maximise the opportunities of the growing demand for mobile banking and is capable of anticipating the financial needs of each individual customer and sending them personal smart recommendations to help them achieve their financial goals.

In Europe, most innovative banks such as **ABN AMRO, CaixaBank** and **BBVA** have developed their own hassle-free banking brands to cater for millennials and digital savvy users. For instance, in Spain, CaixaBank **launched in 2016 *imaginBank***, a mobile banking service that enables users to control their finances, view their account securely within Facebook, or draw money from an ATM without a card and send money to friends using only a mobile number. Similarly, present in the Netherlands, Germany, Belgium and Austria, Moneyou, a brand of ABN AMRO, is a mobile banking service connected to a mobile app called Tikkie. The app can be used by anyone, regardless of who they bank with; it is only necessary that the person receiving the money to have the app. Once the users enter their name, mobile phone number and the IBAN number, they can start sending payment requests via WhatsApp, Facebook Messenger, Telegram, QR-code or text (SMS).

How is my current onboarding process performing – the challengers

Even from the first encounter with the clients, challengers have been praised for providing great user experience. And why is that? They **are digital**, they can develop from scratch, **have smaller product offering**, they do **not depend on legacy systems**, and are **adopting new technologies** to automate identity verification processes.

For example, **Fidor Bank, a German online bank, founded in 2009**, has a simplified, three-stage process of onboarding depending on two essential variables: customer behaviour and product complexity. For the Fidor's Smart Cash Account product, the entry point for a new customer is to join the Fidor community, by supplying one's credentials from Facebook, with no obligation to buy anything. Step two is obtaining a pre-funded online 'wallet' that can be used to move money within a closed loop as the user graduates to being a 'customer' after passing reduced KYC. This allows him or her to test out Fidor, again without any further commitment, while still being part of the community. The third and last step is to open a more traditional account after passing full KYC. Now the customer can also trade commodities, FX, and digital currencies. ➔

An Introduction to Customer Onboarding and Digital Identity Verification

So, the Fidor Smart Cash Account **behaves according to the way the customer registers**, not according to a bank-imposed process.

In general, banks must check the identity of everyone opening an account to prevent money laundering or other criminal financing activities. While these ID checks used to take place exclusively at bank counters, nowadays many services use video identification - customers rotate their ID card in front of a camera allowing staff to check for security features, like holograms - or just selfies.

However, **this simplicity might come at a cost**. **Germany's N26 could be potentially vulnerable to money laundering** and terrorism financing, according to a German publication WirtschaftsWoche, which exposed a security gap at the online banking startup. As the fintech rolled out a selfie validation procedure for account opening, it is easier for criminals to open accounts with fake IDs. A WirtschaftsWoche correspondent saw how a man scanned a friend's ID, added his own passport photo to the ID, printed it out and stuck it atop of a white plastic card that was the same size as the office ID card in his country. He cut the edges to make them round and the result was a new identification card that could be used to open a new bank account.

"Go online or go home" – ways to improve it

INNOPAY developed a Benchmark that provides banks with **essential insights into how to make a good first impression on customers**. INNOPAY consultants have identified six key actions that banks should execute in order to provide the prospective customers the best-possible onboarding experience and increase conversion rates.

1. Eliminate all **channel breaks** to support an end-to-end fully digital onboarding experience. For example, banks should adopt paperless onboarding processes as well as processes for which no physical signature is required.
2. Make required onboarding information and prerequisites **transparent** and understandable for the user. For instance, clear information and communication are key, so that the potential customer has all relevant details at hand and can run through the process in a smooth way.
3. Guide the customer through the onboarding flow and empower **customer support** to help prospects during onboarding in a quick and high-quality manner. The end result is that the prospects always know where they are currently positioned within the process and find information quickly. If they do not understand why the bank is asking for certain information or why the bank requires the prospect to use a certain identification method, they can rely on professional support provided by the bank.
4. Make use of **tools** that ease the process of data entry and eliminate errors. Thus, errors can be prevented by various in-process validation tools to increase conversion and also to reduce manual efforts by the bank, leading to cost reduction.
5. Enable customers to **instantly login** and start using the payment account after a successful onboarding.
6. Deliver a **consistent look and feel** throughout the whole onboarding experience. →

An Introduction to Customer Onboarding and Digital Identity Verification

Overall, we can conclude that banks can stay relevant for their customers if they transform the entire on-boarding process online. So far, we have seen that consumers are more likely to apply for a product if the process is 100% online and if paper-based identity checks are eliminated.

Moreover, the onboarding process could be accelerated if they could use their verified physical ID, such as a passport or driving license, and here, in the 100%-online application process, an important role is played by identity verification.

Identity verification: some last thoughts

Identity verification is proving that specific identity attributes are actually connected to the person, entity, or thing that they are intended to represent. **According to Josje Fiolet**, Digital Onboarding lead at INNOPAY, video identification, reading the chip of the document via NFC (Near-Field Communication), using eID solutions, or taking a picture of the ID document can enable businesses to answer questions such as ‘Is the customer’s document valid?’, or ‘Is the person really who he/she claims to be?’.

To build a reliable profile of the customer, other techniques can also be considered. The trail of data that we leave behind may not be an identification method in itself, but it can serve as an additional step when building a trustworthy profile. For example, our activity on social networks can be used to provide a certain level of assurance of someone’s identity, and the account’s profile picture can be matched with the picture in the identification document.

For effective client identification, a business must have access to a range of technology solutions that can indicate the veracity of an individual along with providing access to worldwide trusted datasets that contain billions of data elements of information from governments/public bodies, including global postal, telecoms and other public data, to validate the underlying data associated with financial services provision. Not only does this deliver a 360-degree view of the individual, but it also authenticates who they are.

The key to all these lies in balancing these elements in order to create perfectly tailored products. By understanding the unique needs of customers, financial businesses can help governments and major institutions fight fraud and grant access to underserved and legitimate customers. We can conclude by underlying one of Money 2020’s ideas from the 2018 edition: once we solve this puzzle of identity custodianship, we can craft a masterpiece in which uniqueness is celebrated, protected and used responsibly.

Trulioo

Hard Problems: Identity Verification, Fraud Prevention and the Giant Leap Towards Financial Inclusion

About Zac Cohen: Zac Cohen is a versatile leader experienced in managing and scaling high-growth companies. Zac is currently the General Manager at Trulioo – a hyper-growth Vancouver startup solving global identity challenges associated with international regulatory compliance, fraud prevention, and trust and safety online. He is passionate about fostering change-makers who want to make an impact and are engaged in building groundbreaking solutions to solve our world's most pressing problems.

Zac Cohen | *General Manager* | Trulioo

At the turn of this decade, the "GDP of the internet" began rising precipitously; online merchants, particularly micro-merchants, began opening online storefronts in increasing numbers. Yet the technology powering the flow of money online was simply not keeping pace. It was this set of unique circumstances that necessitated the creation of a new generation of payment solutions. With their elegantly simple code and their vast network of relationships with credit card issuers, banks and financial services, these payment solutions open the doors to a truly borderless marketplace where online merchants and buyers could transact freely.

A layer of trust

There was, however, another problem that stood in the way: If these payment solutions wanted to enter new markets, particularly unchartered and unfamiliar ones, they needed to first build a layer of trust between themselves and their new customers – the online merchants.

This layer of trust needs to be built on:

- Customer due diligence (CDD): Ensuring a level of CDD that is commensurate with the risks involved in transacting with new customers in these regions. For payment companies, banks, and financial services providers, this includes meeting regulatory requirements such as **Know Your Customer (KYC)**, **Anti-Money Laundering (AML)**.
- Fraud prevention: While the digital economy has created unprecedented opportunities for both established and upstart merchants around the world, it is also prone to fraud. Indeed, prevention is the operative word here, because very often fraud is only detected after the fact.

The challenge

As it happens, the success of both CDD and fraud prevention hinge on a critical process: Identity verification. When it comes to highly competitive and fast-growing companies, it becomes imperative to move quickly and capture as much market share as possible. For these companies, it becomes essential to have an identity verification process that can scale quickly, efficiently, and cost-effectively. In order to do that, these companies need access to a variety of trusted and reliable data sources; but, as it happens, the data that is being sought to verify the identity of merchants in these markets is often available exclusively with local data vendors.

Consider a growing payments company; let's say it is foraying into the Peruvian market. It will likely struggle to forge relationships with local data partners there; it would have to sign multiple contracts with multiple data partners in order to gain access to a sufficiently large swathe of identity data. This process requires a great deal of time, resources and familiarity with the local ecosystem; identifying, procuring, and vetting data sources, and then manually undertaking security and compliance checks. Even from a technology standpoint, the time and investment required to build an API for every data source that the company intends to tap into, become critical roadblocks to their expansion plans. Given these constraints, it would take anywhere between six months to a year for these companies to integrate each data source onto their systems. Now, consider the total time it would take to integrate with multiple data sources across multiple countries; that's when the project begins to look unfeasible. →

The solution: a single API to access identity data across the world

Trulioo has, to a large extent, mitigated this problem; as one of the world's preeminent identity verification solutions, we have access to hundreds of data sources. Through a single API, **GlobalGateway** -- Trulioo's flagship solution -- provides secure access to over 400 data sources across the world. With GlobalGateway, our clients no longer need to sign multiple contracts with multiple parties; instead, a single contract with Trulioo provisions it with access to data from multiple data partners. In fact, one of the world's leading cross-border payroll solutions uses GlobalGateway to verify the identity of payees in 52 countries across different continents, including Chile, Jordan and Egypt.

Instant access to a plethora of data sources also goes a long way in mitigating risk; for instance, companies tend to put off their CDD process till such time as a merchant starts transacting beyond a certain dollar threshold — this is mainly because traditional processes of identity verification were manual, slow and required much human effort. The instantaneity of identity verification, which Trulioo enables, allows companies to place identity verification at the very beginning of **merchant onboarding**; the same instantaneity makes it easy for many of our clients to verify (rather, reverify) the identities of their existing merchants. As a result, our clients are able to understand their entire consumer base quickly and take timely cognizance of any risks that their merchants might pose.

Mobile ID verification: a boost for financial inclusion and an antidote to fraud prevention

From very early on, we, at Trulioo, saw identity verification as a catalyst for financial inclusion; to that end, we realised that we needed to cover hard-to-reach areas, which lacked traditional sources of identity data. As of October, Trulioo can verify the identity of up to **five billion people**, or two-thirds of the world's population, along with 250 million businesses, including micro-merchants. In developing areas of the world, where a large part of the population is "unbanked", and traditional sources of identity data have limited coverage, **mobile network operators** (MNOs) can play a game-changing role. In developing markets, the mobile user base outstrips that of financial services: for instance, over the last four years, over a billion mobile accounts were opened around the world, compared to 500 million bank accounts. Indeed, the data in possession of MNOs can go a long way in verifying the identity of otherwise "thin-file" merchants.

Trulioo
Building Trust Online

About Trulioo: Trulioo is a global identity verification company providing advanced analytics from traditional and alternative data sources to verify identities in real-time. Through GlobalGateway, Trulioo's electronic verification platform, clients are able to streamline their cross-border compliance needs, helping them meet Anti-Money Laundering and Know Your Customer requirements, while simultaneously mitigating fraud and reducing risk.

www.trulioo.com

Click here for the company profile

To that end, **we began partnering** with MNOs around the world. Currently, we have access to identity data provided by dozens of MNOs, which cover 1.8 billion mobile users. When the traditional KYC-compliant sources of data are combined with MNO data, one is able to obtain more insight into the identity that one is trying to verify. No less important is the added value that MNOs bring to fraud prevention; for example, when verifying a merchant's mobile number against MNO data, GlobalGateway can flag numbers that are VoIP numbers, which are often prone to misuse by fraudsters.

We are one breakthrough away from financial inclusion

If we look back at the evolution of online commerce, we realise that at different points, there have been different technological breakthroughs that have catalysed the sector in different ways. The revolution in online payments was one such breakthrough; identity verification is on the cusp of being the next breakthrough. Today, merchants from around the world can transact online as free agents of the online economy; our dream is to see a world where they are able to transact not just as free agents but equals of a financially inclusive ecosystem.