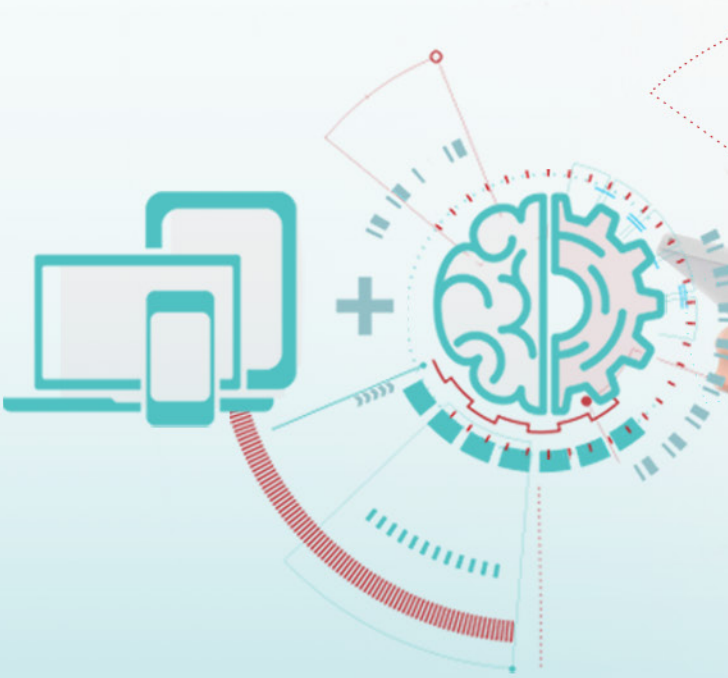
Enhancing Your Customers Digital Identities From The Device Up.

Device Intelligence and KYC for Enhanced Digital Profiling and Optimised Risk Mitigation.



WRITTEN BY:

4STOP + iovation®

Introduction

In today's ever-changing online eco-system that encompasses continuous technology advancements, multiple end-user device implementations and vulnerability to modern fraudsters, the usability of smart technology, like device intelligence and multi-layered KYC are paramount for efficient and successful risk mitigation on a global scale.

4Stop and iovation; leaders passionate about making online engagements not only user-friendly but secure and trustworthy, discuss the importance and benefits device intelligence and enhanced KYC brings to customer engagement and fraud defence.

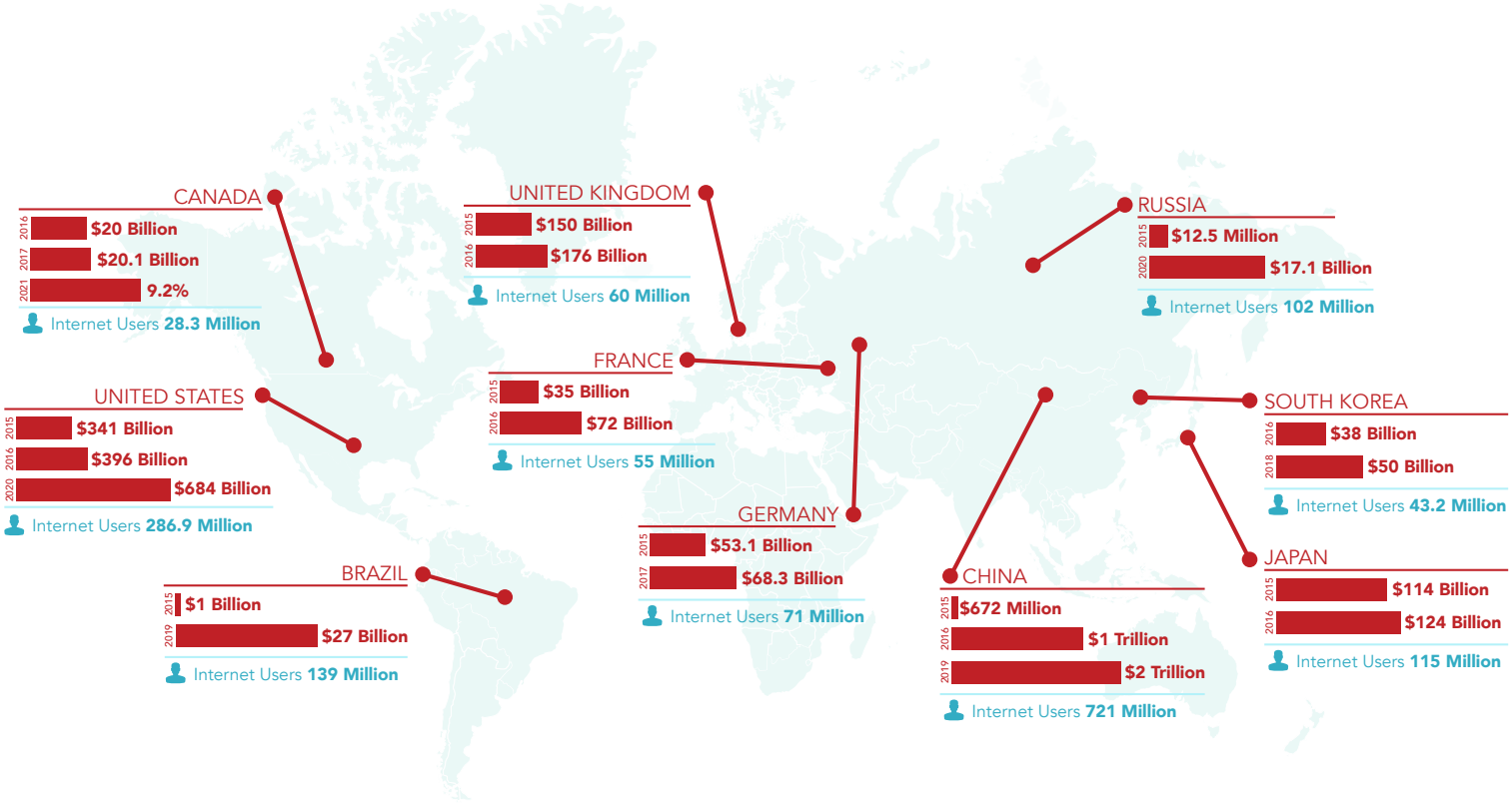
WHAT WE'LL COVER:

1. **Landscape:** A review of the global eCommerce and online engagement trends.
2. **Identity Fraud:** It's a growing concern and leaves 7.3 Billion users online vulnerable.
3. **Device ID to Support:** How to utilise device intelligence to best combat fraud.
4. **KYC & Consumer Trust:** Have confidence in your customers with a multi-factor verification process.
5. **Benefits to VaaS:** Integrating with a VaaS solution dramatically improves operations.
6. **Proven Results:** A look at the numbers on fraud reduction and cost-savings.

Landscape

Global eCommerce is rapidly growing - From $1.5 Trillion in 2015 to an expected $4.5 Trillion in 2021. Non-Cash Next Generation Payment is expected to grow at a CAGR of 10.9% from 2015-2021.

With more growth comes more risk.



Our online world is compromised by the post-breach environment where one or multiple personal customer data information may be compromised in conjunction with sophistication and globalisation of cybercrime fraudsters.

Protecting customers onboarding experience and their associated transactions is truly paramount to the success of any online business. Implementing an array of Know Your Customer (KYC) processes is fundamental to not only ensure risk exposure to enterprise fraud is minimised, but to meet with required regulatory requirements - which are changing dramatically.

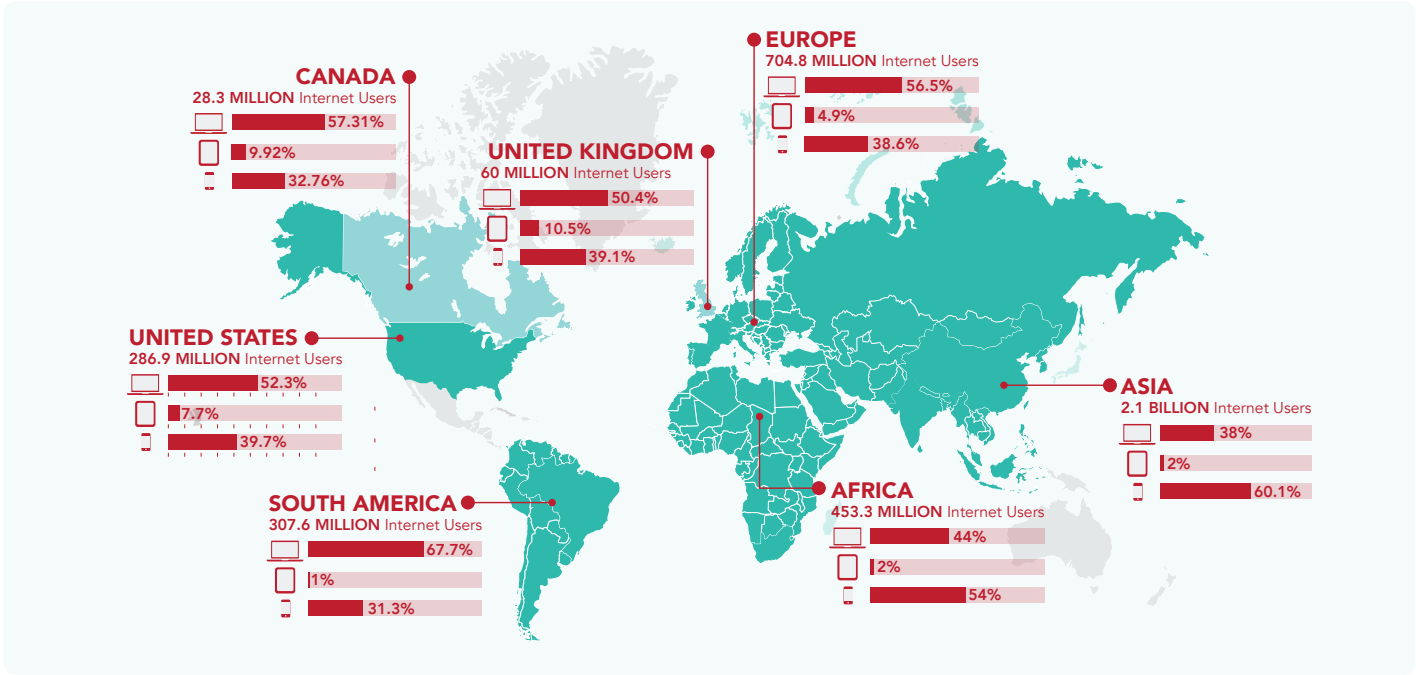
How customers utilise and engage with their devices, locations, patterns and behaviours, transactions, registrations and logins quickly become a vital component to their overall digital identity DNA fingerprint. Which in turn translates down to how they engage with your business products/services online.

The more you know about your customers, the more you not only have trust and confidence in their engagement but can begin to tailor their experiences; building brand loyalty, improving their overall customer lifetime value and obtain revenue retention and business growth.

With a global population of 7.6 Billion with...

7.3 Billion users online.

With most consumers owning smartphone and mobile devices (91 percent), followed closely by laptop computers (83 percent), it is evident that the digital marketplace is here now. Our global technology advancements are performing exponentially with countless solutions designed to support the large volumes of online B2C (Business to Consumer) interactions worldwide; rapidly expanding in volume, expectations, and cross-boarder capabilities. Currently we have an active daily online population of 6.57 billion users and a global adoption of digital commerce with online shopping charting as the top activity on devices (90 percent). It is clear the future of online payment is well positioned for rapid growth and online businesses need to implement the right measures to ensure continued trust in their brand.



Everyday
Users Access Online

Weekly
User Access Online

1/5 Transact
Online Per 30 Days.

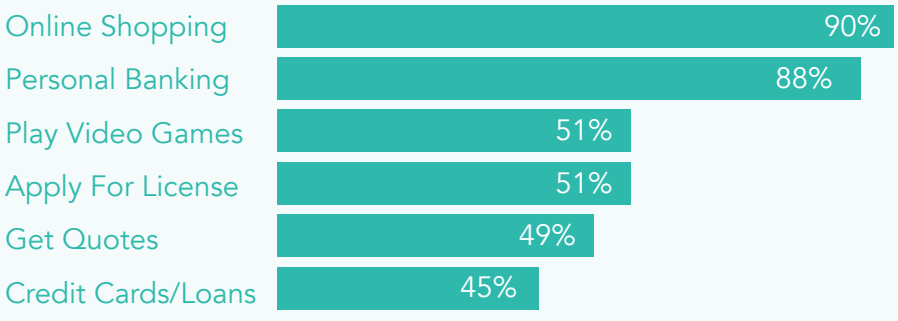
TIME SPENT...

6 HOURS
Millennials 18-34

4 HOURS
GenerationX 35-50

2.5 HOURS
Baby Boomers 51-69

TOP ACTIVITIES...



LAYERED WITH EVOLVING GLOBAL COMPLIANCE.

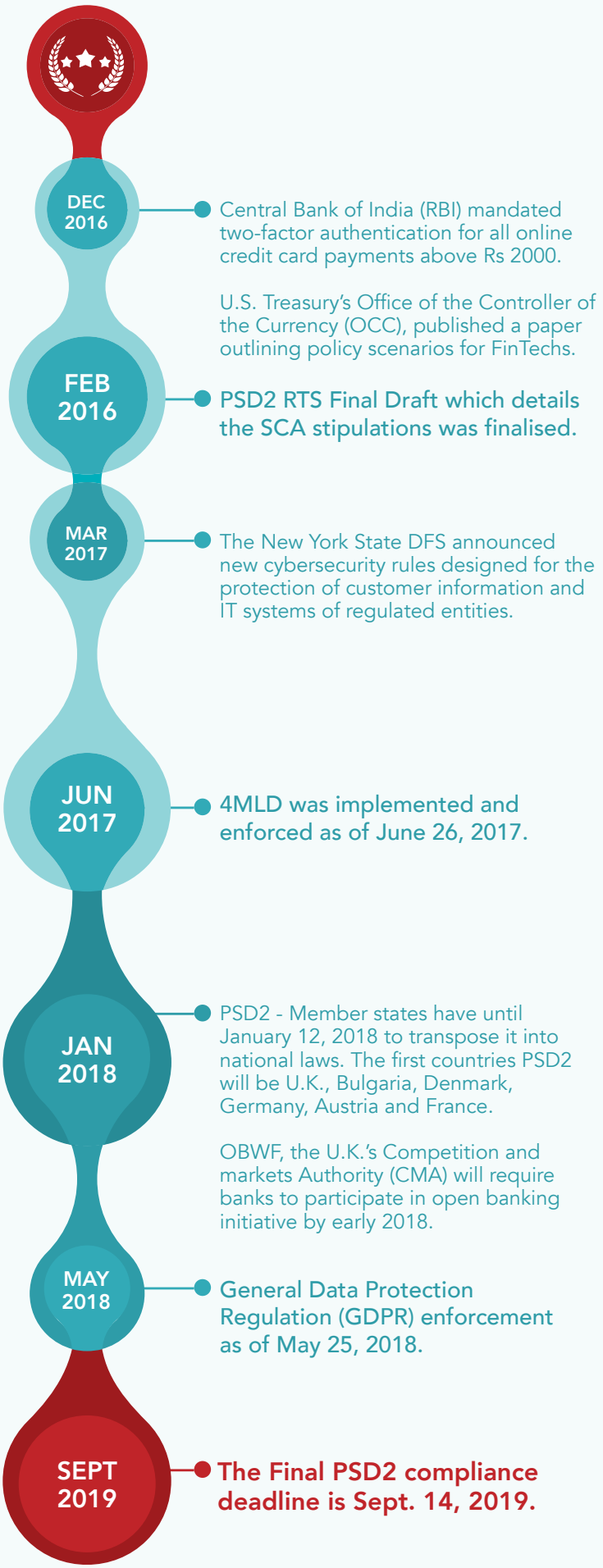
Future-proofing your third-party relationships and your customers, protecting your reputation, and ensuring you comply with the relevant laws and regulations, requires staying on top of your compliance data and measures. However, doing so in a manner that does not come with an array of complexity, loss of time, allocated resources, costs and a cumbersome process, is a challenge in its own.

Know Your Customer (KYC) for regulatory requirements continue to evolve both in the type of due diligence required and the level of complexity in which it is performed; At a per localised region, worldwide and per industry.

Financial institutions (FIs), banks and their customers are constantly managing the ever-changing regulatory landscape and trying to find new streamlined and cost-effective methods to integrate changes when they occur; often times, turning to new partnerships and solutions within the FinTech space.

Business find themselves in an era where simple box-checking with manual due-diligence is no longer acceptable and to enter an age of rigorous, granular, data-driven due-diligence. Ensuring they not only meet compliance for onboarding businesses and their associated customers, but to ensure that their brand reputation remains powerful and untarnished.

While compliance is not an option but a legal requirement, these businesses must integrate processes that satisfy the regulator while still delivering a positive customer experience and maintaining their consumers trust. This is where VaaS (Verification as a Service) providers, data aggregators and verification intelligence providers are vital to their risk mitigation and compliance management equation.



Identity Fraud

It's becoming a serious problem.

In July 2019 there were 2.3 Billion records leaked and cyber attacks.

According to the 2018 identity fraud report Fraud Enters a New Era of Complexity, there were 16.7 million victims of identity fraud, a new record high.

Through exponential global volume of online users, data, and technology advancement, sophisticated criminals are engaging in complex identity fraud schemes, resulting in record high identity theft reportings. In the US alone there were 16.7 million identity theft victims with the cost of the lost data amounting to over nearly $17 Billion. While over in the UK, CIFAS reports that almost 500 identities are stolen every day.

In 2017 compromised social security numbers exceeded credit card numbers for the first time, driving an increase in identity fraud.

IDENTITY FRAUD

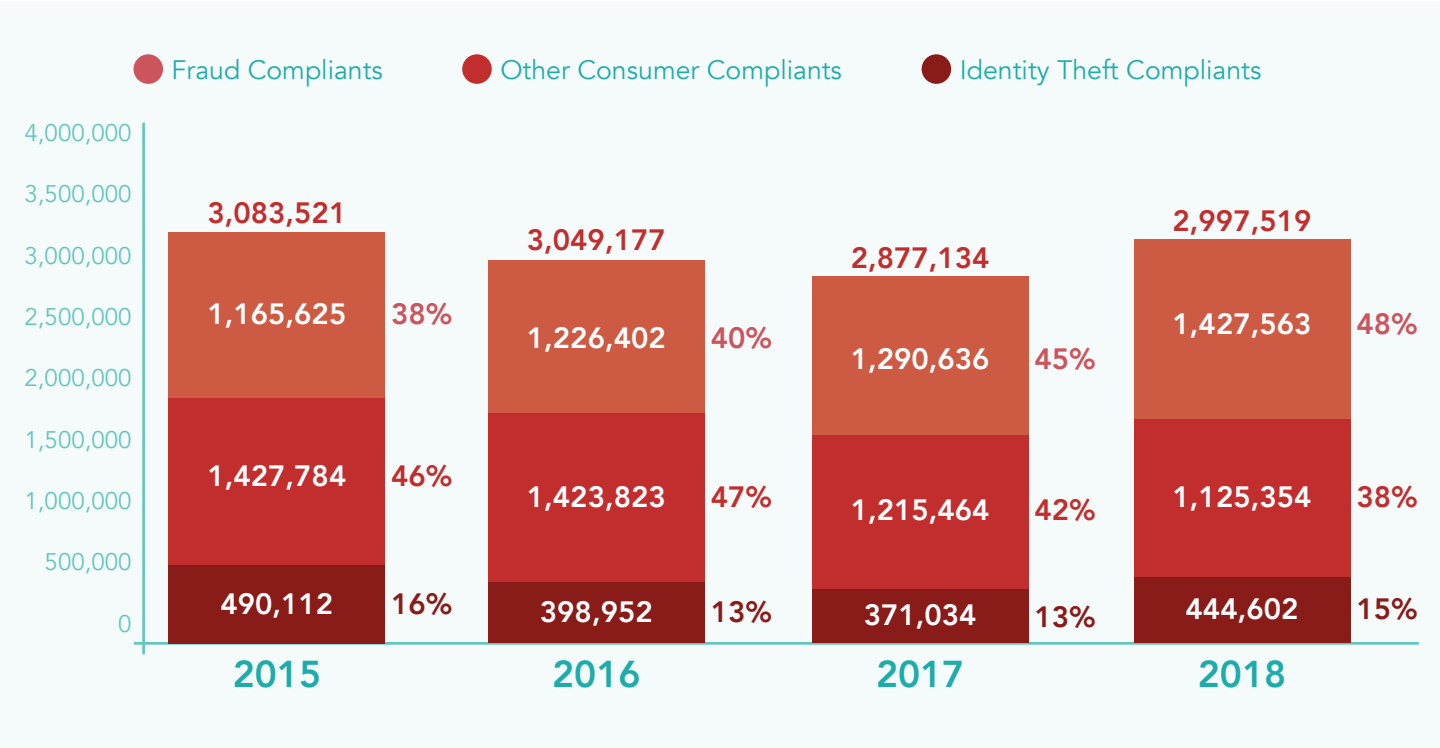
The unauthorised use of someone's personal information for illicit financial gain. Identity fraud ranges from using a stolen payment card account for a fraudulent purchase to opening fraudulent new accounts.

IDENTITY THEFT

Unauthorised access to personal information. It can occur without identity fraud, such as through data breaches. Once theft is used for illicit financial gain, it is then considered an identity fraud.

This rapidly growing cyber vulnerability places enhanced pressure on businesses to ensure the appropriate fraud defence measure are in place to mitigate risk at the point of consumer entry. A focus that is not only relevant for the success of their business revenues, but the trust of their customers. Four out of five consumers trust that businesses are not only making the appropriate cybersecurity measures to ensure their personal data security, but that it is a top priority.

Criminals are focusing on new account fraud following the introduction of microchip equipped credit cards back in 2015, which make the cards difficult to counterfeit. New account fraud occurs when a fraudster opens a credit card or financial account using an identity theft victims name and other stolen information. *Account takeovers is the fastest growing identity theft method. In 2018 it grew by tripling from the previous year, reaching a four-year high and experienced losses of $5.1 Billion.*



TOP 5 IDENTITY THEFT FRAUD, 2018

#1 **Credit Card Fraud**
New Accounts
Reports Received:**130,928**
40.5%

#2 **Miscellaneous Identity Theft**
Payment Fraud, Email, Social*
Reports Received:**87,765**
27.1%

#3 **Tax Fraud**
Reports Received:**38,967**
12%

#4 **Mobile Telephone**
New Accounts
Reports Received:**33,466**
10.3%

#5 **Credit Card Fraud**
Existing Accounts
Reports Received:**32,329**
10%

Consumers can report multiple types of identity theft. In 2018, 17 percent of identity theft reports included more than one type of identity theft.

**Includes online shopping and payment account fraud, email and social media fraud, and medical services, insurance and securities account fraud, and other identity theft.*

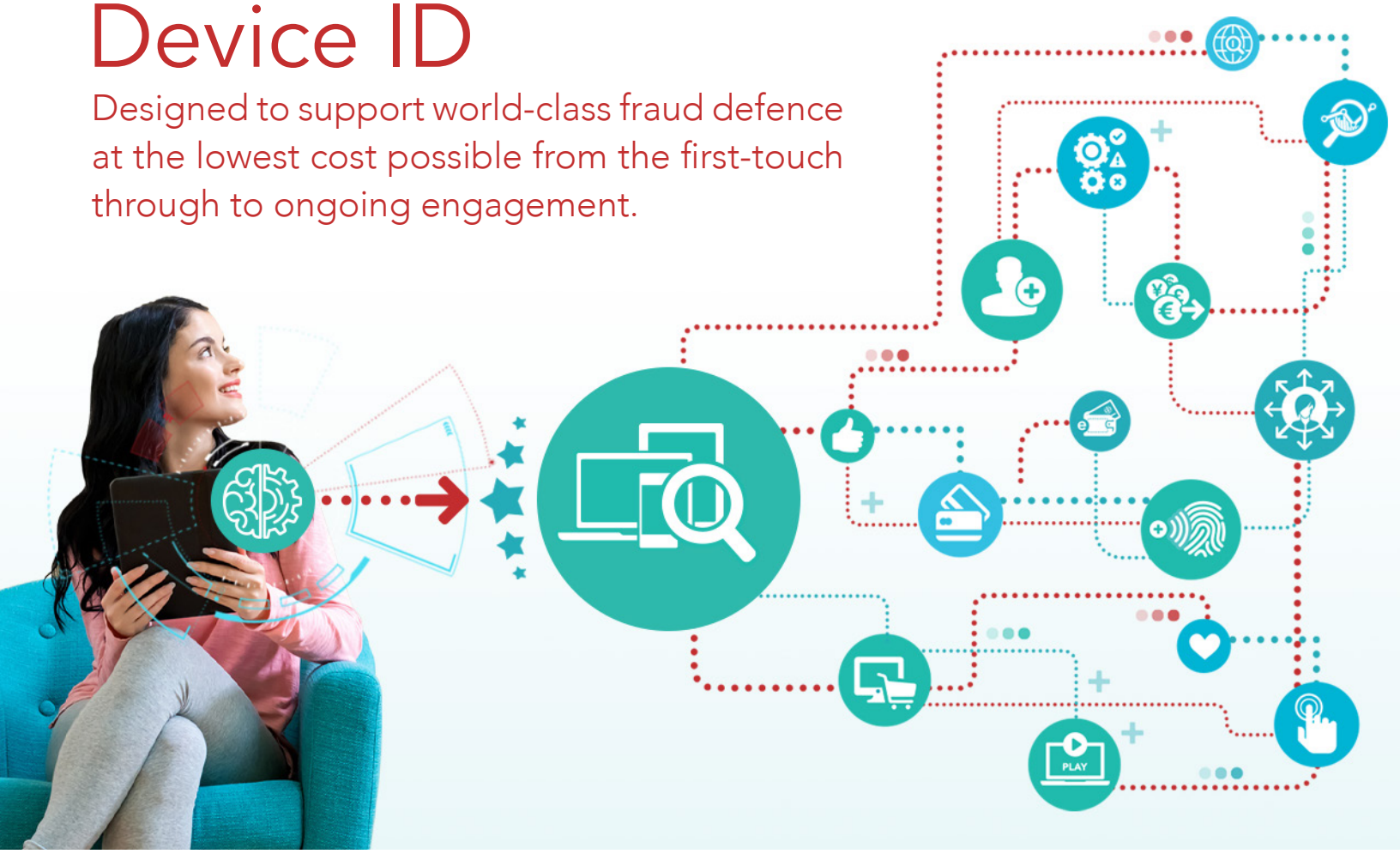
Device intelligence is a core foundational fraud defence tool. Understanding and utilising this intelligence does more than just complement AML KYC compliance checks, but maximises fraud defence for everyone who engages online.

- Providing passive two-factor authentication for online transactions without requiring software, hardware tokens or knowledge based challenge questions.
- Not relying on the collection of personal identifying information (PII)
- Stops first-time fraud attempts based on device anomalies and global behavior.

In conjunction with device intelligence, online businesses should look at the benefits of layered KYC (above what is required for compliance) to truly combat fraud and protect their business with confidence. Data-driven dynamic KYC as part of onboarding and transactional security measures dramatically cuts the cost of fraud and positions businesses for accelerated growth. Working with a VaaS provider or KYC data aggregator makes obtaining KYC on a global scale quick and easy, with nearly zero touch on business operations.

Device ID

Designed to support world-class fraud defence at the lowest cost possible from the first-touch through to ongoing engagement.



Since the first generation of device identification technologies were introduced the global online landscape has changed drastically and basic Device ID is no longer enough. It is imperative to layer Device ID with advanced combining recognition technologies and anti-fraud tools.

Adopting a Device ID provider with a layered approach when detecting and preventing online fraud and abuse in real-time gives the financial industry an advantage to combat various types of fraud such as:

- New Account or Application
- Account Takeover
- Policy & Abuse Violations
- Stolen &/or Synthetic Identity
- Loans Defaults
- Payment Fraud

While fighting fraud, you are also building consumer trust throughout their journey; from creating an account to their transfer of funds. A device layered approach reduces the risk in each integration point of a customer's journey and records the Device ID evidence.

Having access to good, complete data that performs in an automated, dynamic and real-time manner businesses can onboard their customers and verify associated transactions with absolute confidence.

Of businesses want advanced authentication and security measures that have little or no impact on the digital customer experience.

Consumer Trust

Building trust through technology without disruption is increasingly the goal, but also the responsibility of businesses with online channels. While there are genuine barriers to achieving that goal, it is more critical than ever for business to outcome. Businesses need to look beyond just implementing KYC for compliance and utilise KYC data to enhance customers digital profile, experience and trust.

Fraud Detection & Prevention Methods

- **49%** Security Questions
- **52%** Password Protection
- **50%** Account Set Up Measures
- **49%** Credit Card Security
- **45%** PIN Codes
- **44%** Multi-Factor Authentication
- **40%** Document ID Verification
- **35%** Knowledge Base Answers

Nearly two-thirds (66 percent) of consumers appreciate security protocols when transacting online because it makes them feel protected.

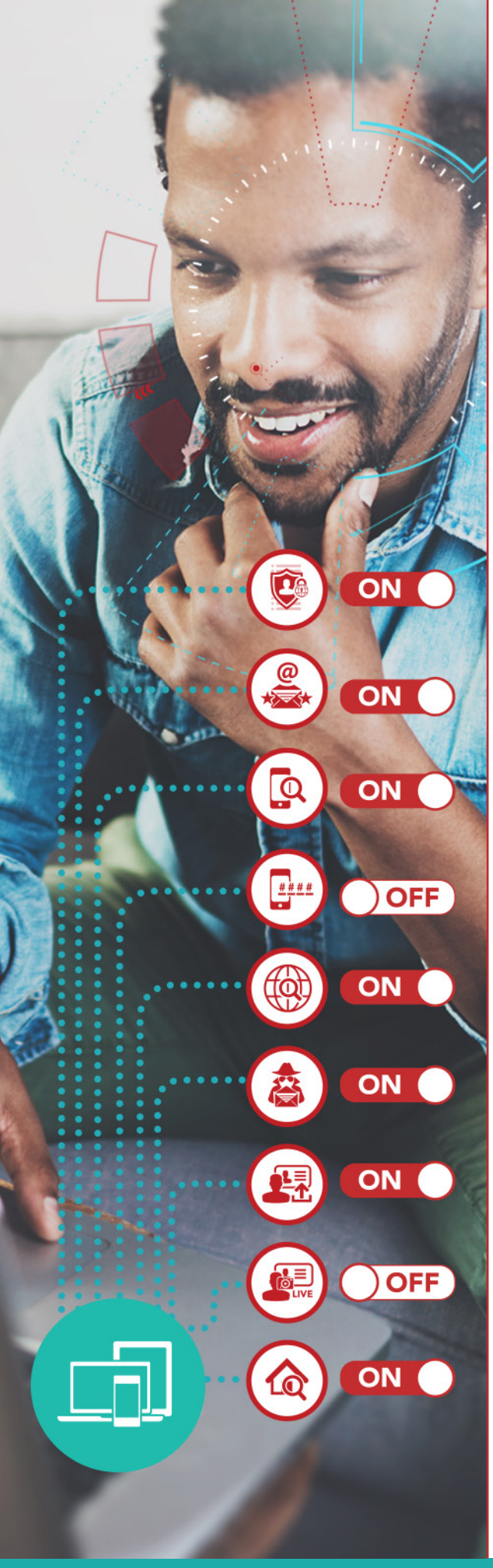
Of customers appreciate the extra security process when they engage.

Lack of visible security is the number one reason customers abandon an account creation or transaction. Resulting in a loss of 27% of transactions in 2018.

With this figure we can take a strong assumption that even though today's online engagement demands frictionless and automatic results the tolerance for friction for the sake of security is rationalised. Consumers tolerate the nuisance of common barriers to accessing their accounts such as forgetting passwords, pin codes, selfies, knowledge based questions, or other security protocols. They conclude that higher friction can also be indicative of stronger security to protect their experience and digital identity.

Device ID intelligence should be at the core of every online fraud prevention process. From pre-screening customers to every login, account update and transaction, obtaining the device fingerprint, behaviour patterns and association logic is the quickest and most cost-effective KYC to identify when risk exposure is occuring.

84% of businesses said that if they were certain about a customers identity, the need for fraud risk mitigation would be reduced.



Ultimately the only way we can currently onboard customers and then verify every transaction is by having good data.

Whether your facilitating eCommerce, built an eWallet, are part of the digital financial Crypto evolution or are a Payment Service Provider, we now live in a world where facilitating these customer accounts and transactions needs to live up to the expectations of the end users. Everyone expects instant results and immediate gratification. Customers today have high expectations and demand the ability to create their account and be approved for transactional processing in real-time. However, the only way to easily obtain this level of verification performance is for businesses to have access to good data points with the ability to effortlessly manage those data points and linking that data to automated, real-time fraud prevention technology.

For a lot of businesses obtaining this is quite a cumbersome, timely and costly process. Implementing thousands of new data solutions at say $10K per solution entry to have reserve on account or access to data simply puts too much strain on individual business resources and impacts their overall performance. As a result many businesses opt to only implement KYC for their regulatory obligations and sacrificing the greater opportunity that performing multiple KYC can do for their business.

Enhancing customers profiles with KYC at various touch points of a customer journey results in 'good' customers entering the system through to ensuring transactions are being processed as good, efficient and accurate as possible, all of the time. If businesses can identify intimately with their customers digital identities they can accelerate their business performance and revenue retention.

- Dramatically reduce fraud and its associated costs
- Allow customers higher transactional threshold volumes
- Improve authorisation rates
- Reduce chargebacks and friendly fraud rates
- Improve their reaction times to sight fraud before it occurs
- Improve their customers trust and life-time value

Validating, verifying and authenticating each customer and transaction varies tremendously. The reality is for a transaction to run efficiently around the world, you need a wild assortment of different data points to be called upon in a certain manner and to be as fluid as possible. The only way to obtain this without integrating endless data points and managing 3rd party KYC integrations is through data aggregation.

Thankfully through our evolving FinTech and RegTech, businesses can easily work with a VaaS (Verification as a Service) provider to obtain all the global data services they require to meet their KYC, AML and GDPR compliance obligations. Additionally with access to a suite of KYC on reserve for enhanced digital profiling.

BENEFITS OF A VAAS

- Hundreds of KYC
- Cost-Efficient
- On-Demand KYC Ability
- Single API Integration
- Global KYC Coverage
- Reduced IT Time
- Enriched Data Obtained
- Quicker to Markets

Businesses that have combined enhanced KYC digital profiling with smart anti-fraud technology experienced an average of 82% approval authorization rate.

Businesses that have combined enhanced KYC with automated anti-fraud technology experience a 67% reduction in charge-backs in the first 2 months.

"When businesses transact globally in real-time, the potential for fraud is a lot higher as often times they don't have the ability to review the volume and speed of onboarding registrations and transactions.

An online business can have up to 2,000 data parameters for a single transaction. If you multiply that by millions of transactions per day or sometimes even per hour, it's tough for global companies trying to achieve instant payments under PSD2, for instance, to stay on top.

It's an irony that, in an era requiring tighter controls, open banking has potentially increased companies' exposure to risk. And yet it is quite essential they do stay on top of compliance and mitigating risk in order to not make thousands of customer accounts hvulnerable to cybercrime.

Partnering with a global KYC data aggregator that performs your KYC in real-time and pairs it with data- driven fraud defence allows for a centralised view of risk to improve reaction times and drive a positive brand experience."

Ingo Ernst, CEO
4Stop

Conclusion

Utilising Device ID intelligence layered with an array of diverse KYC technologies will enhance digital profiling and maximize fraud behaviour mapping. Allowing you to easily combat fraud and bring trust to every customer and their associated transactions on a global scale.

The sheer current and expected volume of our online transactional eco-system in conjunction with our trends of online fraud and identity theft demands businesses to facilitate a modern approach to their risk management processes. Enhancing customers digital profiles through the right technology is ultimately the fail-safe approach at mitigating risk.

Utilising KYC solutions that prescreen on first layer fraud detection like Device ID intelligence in conjunction with an array of KYC verifications has been proven to empower businesses to make decisions backed behind quantifiable data. Allowing them to harness the confidence and trust the data provides and improve their customer retention and profitability.

LEARN MORE

Watch COO of 4Stop Nolan Bolusan and EVP, Global Sales of iovation Tom Pak, as they deep dive into the topic of device intelligence and multiple KYC for enhanced digital profiling.

WATCH NOW

About The Authors.

4STOP

4Stop, was founded in 2016 to solve businesses global risk-based approach through a modern, all-in-one KYB, KYC, compliance and anti-fraud solution from a single API. 4Stop's technology creates an unrivaled combination that allows businesses to confidently anticipate risk and be empowered to make well-informed decisions, backed by quantifiable data to manage regulatory obligations that will accelerate their business performance. 4Stop has been developed with a full understanding of global compliance needs — locally and globally, today and in the future.

To learn more visit https://www.4stop.com

Contact directly at info@4stop.com I sales@4stop.com

---

iovation
A TransUnion® Company

iovation, a TransUnion company, was founded with a simple guiding mission: to make the Internet a safer place for people to conduct business. Since 2004, the company has been delivering against that goal, helping brands protect and engage their customers, and keeping them secure in the complex digital world. Armed with the world's largest and most precise database of reputation insights and cryptographically secure multi-factor authentication methods, iovation safeguards tens of millions of digital transactions each day.

To learn more visit https://www.iovation.com/

Contact directly at info@iovation.com I sales@iovation.com

RESEARCH RELATED

Fraud Management Insights 2017: Trust, Identity and Engagement in a Digital World, Experian APAC

Annual Fraud Indicator Report 2017, Experian UK

Federal Trade Commission, Consumer Sentinel Network

Identity Theft Resource Center

Federal Trade Commision - Top Frauds of 2018