Shufti Pro

Identity Verification

On-premises Identity Verification for the Banking Sector

What’s Inside

The Global Banking Landscape in 2021

Over the past few years, the financial services industry has been on a roll, embracing smart technologies, successfully adapting the COVID-driven trends, and delivering a purposeful experience to consumers. In this regard, top-tier financial institutions (FIs) like banks have pioneered technological disruption, creating more opportunities for ***FinTech*** to flourish. When it comes to digitisation, it plays a key role in making banking operations effective, and secure. On the downside, understanding high-end solutions and integrating them with existing systems remains a challenge.

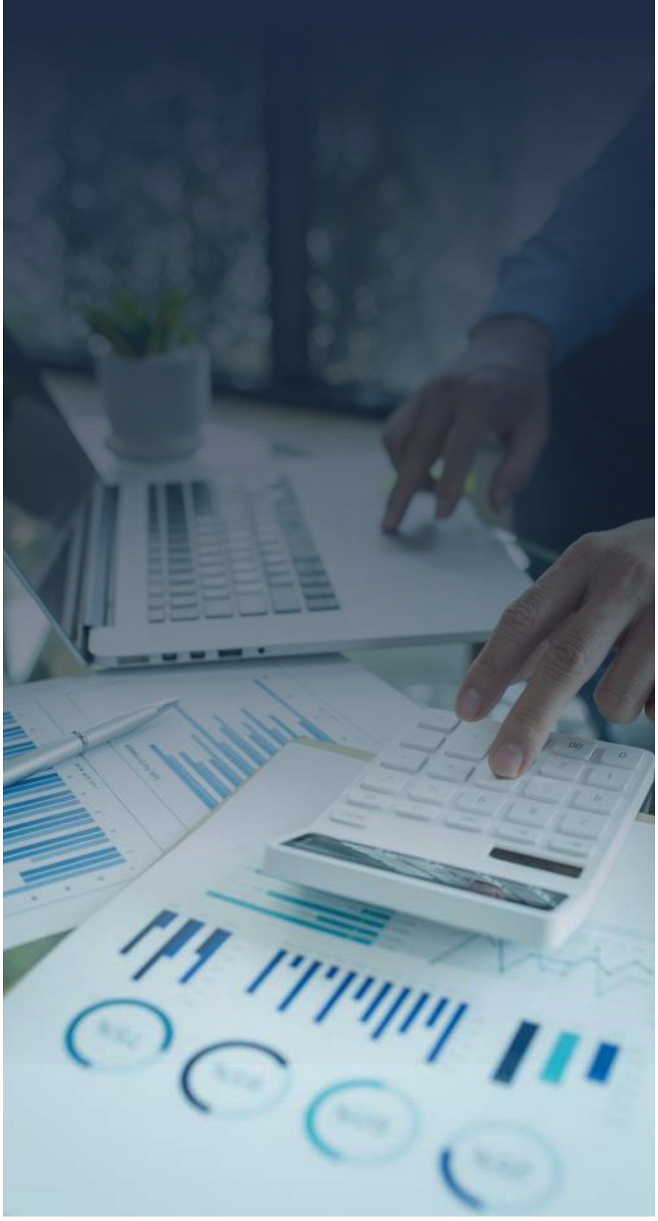
That being said, banks are steadily incorporating digital services in their business models, given the emerging customer needs and the mounting demand for regulatory compliance. To come up with a feasible approach, banks started embracing regulatory technology to fulfil compliance criteria as well as to meet the remote banking needs of customers amid the pandemic.

The COVID-19 Aftermath & More

Before the global health crisis, banks maintained a steady capital ratio that helped the global economy survive through trying times. For banks, the COVID-induced upheaval was not as severe as the 2008 financial crisis, however, it took a toll on the global banking industry in different dimensions making the market even more competitive. Despite the arrival of the vaccine and social distancing measures, the financial services sector still has a long way to go to recover from the drastic impact.

This increasing financial contraction amid COVID-19 has an adverse effect on the volume of payment transactions performed worldwide as well as the loan growth. Moreover, since digitisation is inevitable, especially when contactless experiences are highly prioritised, some perpetrators are seeking different means to take over the financial accounts of online users. As a result, regulatory authorities have raised concerns over the increasing financial crimes, calling for better cybersecurity and *anti-money laundering* (AML) measures.

The IMF's study on the global economic context suggests that although a possible rebound is expected in 2021, the global GDP is forecasted to be under USD 9.3 trillion.[1]



[1] World Economic Outlook - IMF

The global banking sector has timely recognised the need for robust policies and procedures to combat digital fraud, standardising Know Your Customer (KYC) and adopting emerging technology trends. Identity theft, privacy-based concerns, and protecting customers' personally identifiable information (PII) remain the key challenges alongside delivering a seamless customer experience in 2021. To cater a viable solution to these problems, this report discusses "***on-premises identity verification***" which, depending upon the banking needs, offers stronger data residency, authorised access, and a greater sense of security for the customer.

COVID-driven Global Trends

Digital Services

Social safety protocols driving contactless experiences through digital banking

Workforce Virtualization

Banks introducing flexible and remote working models for employees

Corporate Social Responsibility

Banks are redefining strategies amid the pandemic for the greater good

Precautionary Measures

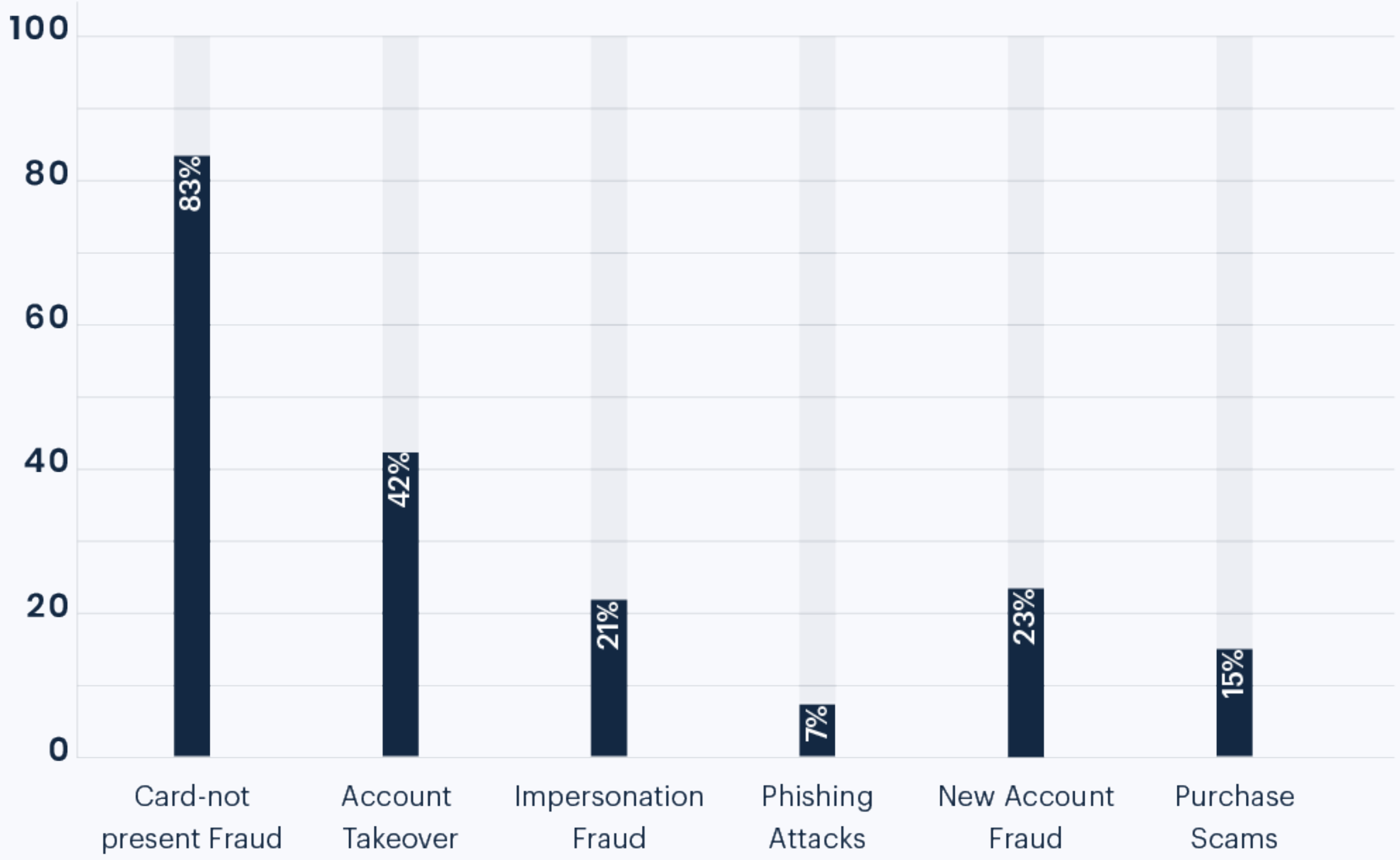
Consumer safety and surveillance is increasing for banking and financial entities

Banking Fraud - Unveiling the Untold Truth

Digital fraud cases, as a result of people falling prey to money-transfer plots, have mounted to 71% in the first half of 2021.[2] Moreover, 93% of banking frauds carried out between the last three months of 2020 up till the Q1 of 2021, were digital, as per a financial crime report.[3] Another study shows that banking fraud grew by 159%, the surge in cross-border payment transactions and consumer interest towards digital services being the main reasons.

Account Takeover (ATO) happens when an intruder gains access to someone else's account using their stolen banking log-in details or creating synthetic personal identity information to deceive the system. Moreover, impersonation fraud involves a fraudster pretending to be someone they are not, typically deceiving the bank through social engineering tactics. Above all of these cyberattacks is the card-not-present (CNP) fraud conducted through online and mobile platforms.

The Ratio of Cyberattacks in Banking



[2] 2021 Bank Transfer Fraud Losses

[3] Banking Fraud up 159% - Info security Magazine

Capitalising on Technology Trends to Combat FinCrime

The banking sector was growing by leaps and bounds before the COVID-19 pandemic, given the rapid digital transformation. Since its onset, online services saw a heightened interest due to a growing demand for contactless services and social distancing obligations. Consequently, banks started accelerating their digital transformation to adopt COVID-led trends to survive market competition, keeping intact the new restrictions.

Since banks needed to develop solutions quickly, this left certain loopholes in security systems and customer onboarding criteria redefined. Four out of five respondents reported that COVID-19 unveiled limitations in their organisation's digital infrastructure, as per the research by Deloitte.[4] The study further elaborates technical debt as a potential barrier while normalising digital adoption in banks and financial institutions. While on a larger scale, digital inertia has withered, the appetite for tech-driven transformation in core systems has increased. In this regard, on-premises solutions deployed at banking sites can enable FIs to overcome functionality, security and service delivery gaps.

Building Resilient Systems

Losses incurred as a result of cybercrime are expected to garner $6 trillion in sum annually by 2021.[5] To address increasing customer concerns, better

[4] 2021 Banking and Capital Markets Outlook - Deloitte

[5] Cybercrime to Top $6 trillion in 2021 - Cybersecurity

maintain regulatory scrutiny and enhance user experience, banks need to strengthen their technology infrastructure. While developing robust systems, capacity constraints should be taken into account, especially in COVID times when people need to maintain safe distance. As a result, AI-powered solutions for verifying customer identity, smart bots for conversational assistance, and enhanced security mechanisms are becoming mainstream.

Risk Assessment Architecture

Regulatory watchdogs around the world keep a vigilant eye on global financial markets and their ever-changing landscape. Owing to the current context, many have introduced stringent regulations that are better aligned with risk assessment and global AML/CFT standards.

To effectively comply with global laws, banking entities started employing ***RegTech*** (Regulatory Technology) solutions for ongoing monitoring, better risk management, and reduced loads on banking personnel. As of now, many service providers in the market offer ***AML screening*** and ***KYC verification*** services that allow banks to sustain operational stability, carry out strategic cost planning, and use data analysis to make informed decisions.

On-premises Vs Cloud Services - What's Better and When?

Cloud-based services have seen increased popularity over recent years due to the ease of integration, scalability and cost factors. However, depending on the business needs, especially those of major financial institutions like banks, on-premises solutions can prove much more effective in terms of data security, privacy and access control, and regulatory compliance. Below is a *comparison of on-premises and cloud services* for the banking sector considering different parameters.

Data Security

68% of business executives feel that cybersecurity risks for their companies are increasing constantly, as per the report by Accenture.[6] For businesses, and banks, in particular, customer data and their financial information is of prime importance. Protecting the digital identity of users has not only become a corporate responsibility but a regulatory obligation as well, which is why top-level FIs are more concerned about in-house data residency.

On a global scale, a single data breach costs as much as $3.9 million

When it comes to cloud storage, customer data is processed and handled by a third party. This possibly increases the risk of unauthorised personnel accessing user data, resulting in

[6] The Cost of Cybercrime - Accenture

external data breaches. In this regard, businesses are now incorporating security policies and procedures that are better aligned with data encryption standards and safe information sharing. Shufti Pro, a UK-based IDV service provider and a *GDPR-certified* entity, addresses these concerns by practising ***customer due diligence*** in light of global data protection regulations.

On-premises IDV

Regulatory authorities require banks to include know your customer and anti-money laundering requirements in their regular customer onboarding procedures. That being said, on-premises identity verification systems offer a viable solution. On-premises solutions offer a seamless method to screen potential customers and are not accessible to anyone outside the company's network. Since data resides on in-house servers, it makes customer information less prone to third-party intrusions. On-premises IDV services are a preferred option for banks and other entities operating in the financial services industry since they need to handle sensitive data daily.

Cost and Speed

Cloud services offer flexible pricing plans based on business needs and are well-suited for startups and SMEs. This allows businesses to manage their capital expenses through an affordable monthly subscription and adjust their budget accordingly. On the other hand, cloud-based service costs can balloon with little to no warning, given the need for rapid scalability and fast-internet connection. This can, however, be properly managed by diligent planning and policymaking.

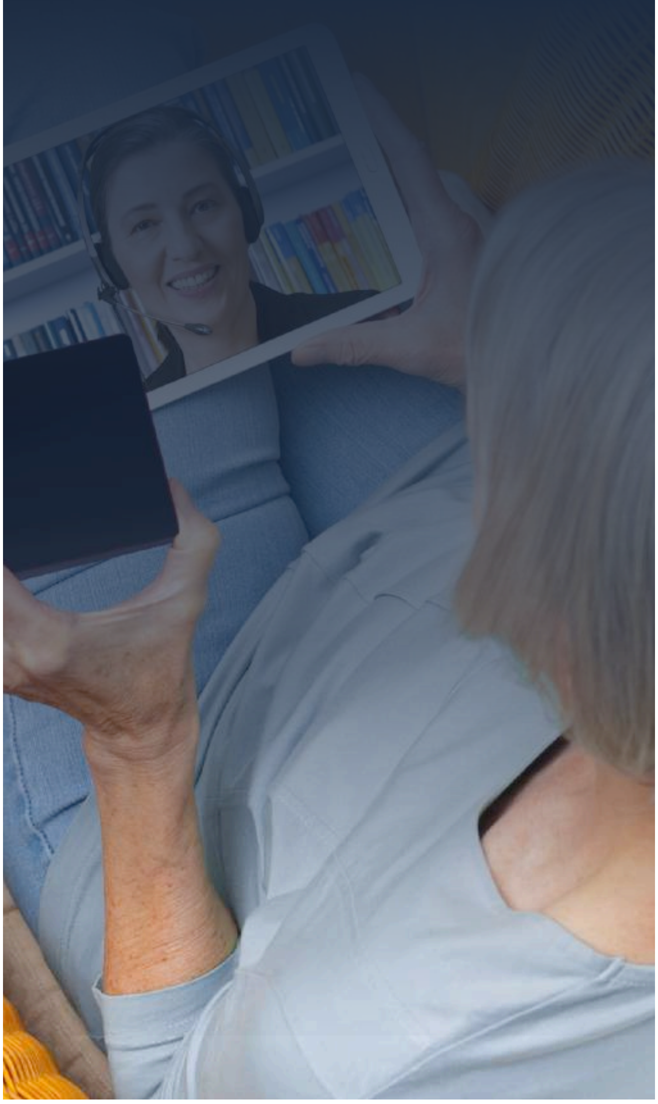
While deployment and maintenance costs for on-premises servers can often be pricey, the long-term benefits outrun the short-term cost. Recurring fraud losses and non-compliance penalties add fuel to fire when it comes to managing financial spendings for businesses. On-premises systems address these challenges by maintaining a data storage repository that is centralised, leaving less room for inter-party perpetrators to hijack information. This brings better financial stability in the long run, particularly for banks that handle sensitive data regularly.

Owing to this, entities operating in the banking sector focus more on data integrity rather than the service cost. Despite the performance and cost challenges, banks operate in the highly regulated financial industry, putting ***KYC/AML compliance*** top of the list. An on-premises IDV solution strikes the perfect balance between strong data residency and effective service delivery to the end-user.

Accessibility & Customization

Without a doubt, cloud-based identity verification services can enable banks to instantly verify clients, keeping intact industry-centric regulations. However, the user experience, in most cases, is tied with the reliability of the remote connection that can directly impact how a business accesses and manages data files and sensitive user information. On the downside, the access is majorly dependent on the internet connection, which could often come at the cost of compromised productivity. Furthermore, cloud services are sometimes less flexible and customizable since they are developed for the industry rather specific to the business.

Shufti Pro, allows businesses to create a dedicated *Hosted Verification Page* (HVP) with additional data parameters for KYC verification, UI/UX customization, and a unique URL



Since banks are highly regulated institutions, an on-premises identity verification solution could offer wider support for their complex architecture needs. Complying with the data-sensitive industry regulations and verifying customers in a secure on-premise environment is all that a banking entity requires. While customizing service features and authorised accessibility impact the overall customer journey, regulatory compliance needs and building that all-important customer trust is equally important

A Case of Third-party Data Breach - Morgan Stanley Bank

The US-based investment banking company, Morgan Stanley, fell prey to a major cyberattack data breach in July 2021. As per the details, the data breach occurred after Accellion's legacy File Transfer Appliance reported a series of supply chain attacks leading to extortion carried out by the Clop ransomware group of cybercriminals.[7] In a formal letter to the New Hampshire Attorney General, Morgan Stanley stated that it experienced an inter-party data breach after a vendor providing services for stock management to the company's employees was compromised.

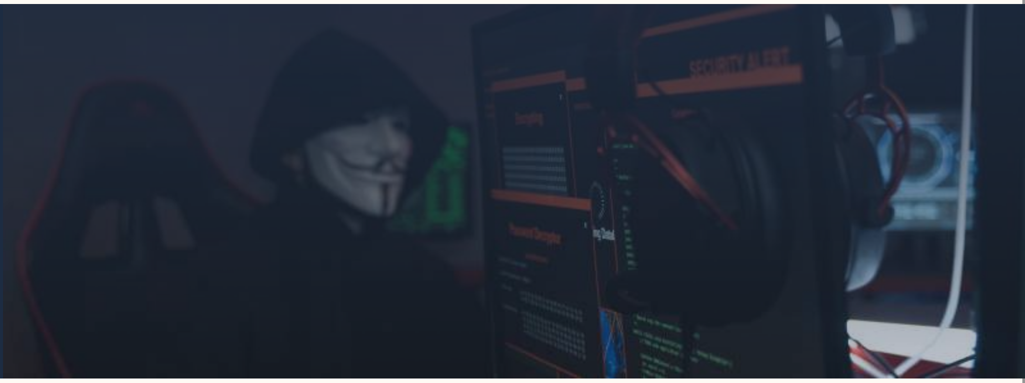
The stolen identity information included names of the victims, addresses, social security numbers (SSNs), dates of birth, and some corporate company names. Earlier, the bank was fined $60 million in October 2016 by the Office of the Comptroller of Currency (OCC) for failing to comply with data protection standards while withdrawing data off of their servers via a third party.[8] This is another example of a failed risk assessment that could have resulted in third-party data extortion.

How Shufti Pro's On-premises IDV Can Help?

The first thing bad actors would do after breaching a system is gain access rights of the privileged accounts. ***Shufti Pro's On-premises Identity Verification Solution*** adopts a zero-trust architecture, enabling banking customers to breeze through Know Your Customer (KYC) procedures while sustaining global regulatory compliance.

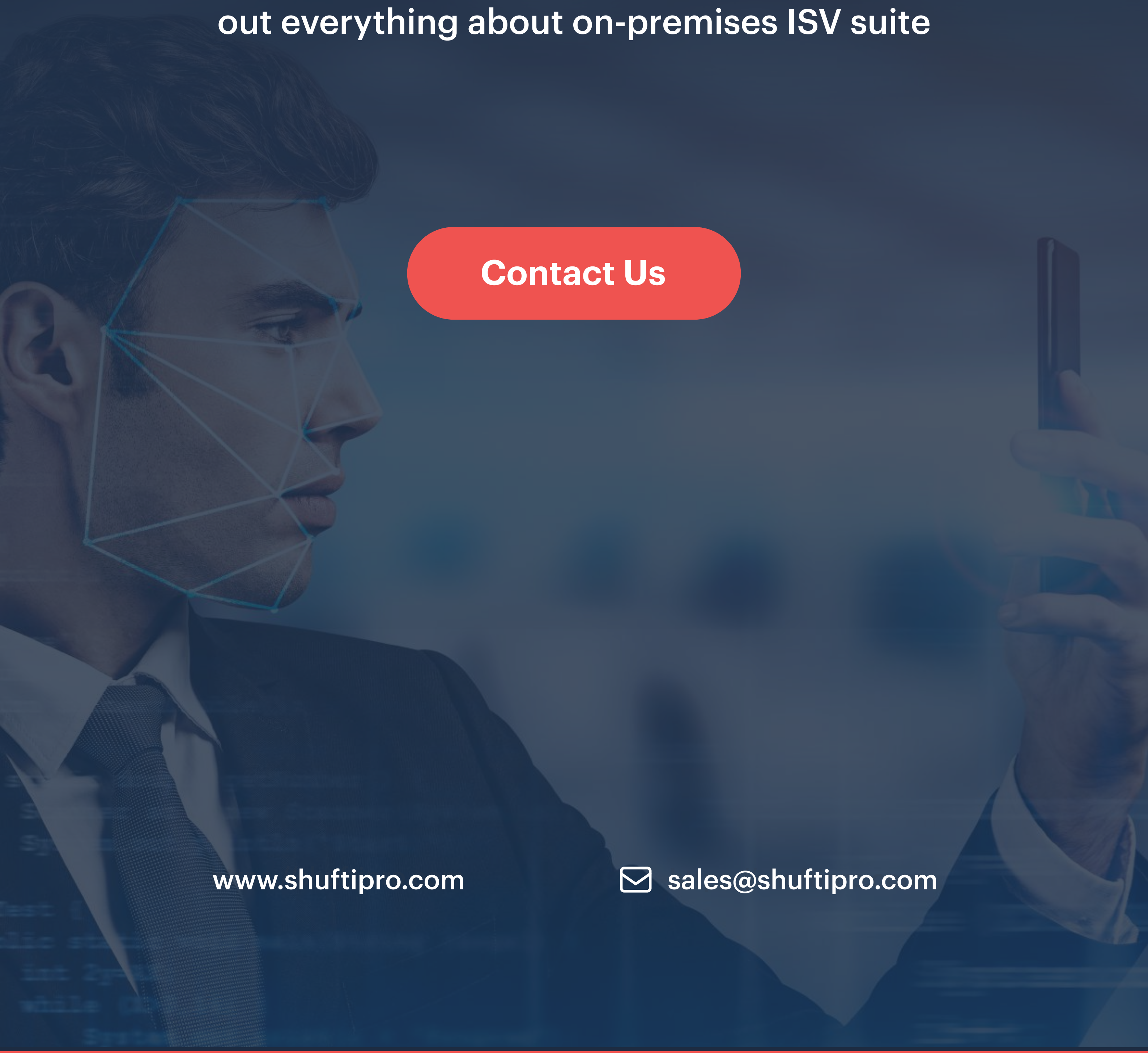
The on-premises IDV service offers strong data residency with complete control over customers' data without third-party intercession. Shufti Pro's comprehensive on-premises suite incorporates multi-tier verification that addresses all banking needs under one roof and ensures strong customer authentication. This allows banks and FIs to develop high data protection and privacy standards as well as trust and transparency with customers and other business entities.

Identity thieves hijacked the encrypted data of 108 New Hampshire residents along with decryption keys for the files, leaving Personally Identifiable Information (PII) of many at stake



[7] Morgan Stanley Joins the List of Accellion FTA Hack Victims

[8] The Lingering Effects of the Accellion Breach



Are you a bank or financial organisation looking for a real-time and resilient in-house solution for customer identity verification? Get in touch with Shufti Pro’s experts to find out everything about on-premises ISV suite

Contact Us

www.shuftipro.com ✉ sales@shuftipro.com

Shufti Pro

Shufti Pro True Identity Builds Trust

Expanding services to 230+ countries and territories in a short period of time, Shufti Pro envisioned playing a pivotal role in creating cyberspace where every transaction is verifiable and secure. With enough experience in technologies like machine learning (ML), OCR, artificial intelligence, and Natural Language Processing (NLP), Shufti Pro strives to provide the best identity verification services to verify customers and businesses online.

Shufti Pro's cost-effective solutions help businesses to prevent fraud and illicit crimes that can ruin the integrity and brand reputation of your business. Our perfect solution suite consisting of KYC verification, AML screening, ID verification, Facial Recognition, Biometric Authentication, Video KYC, OCR, and KYB helps to improve your company's fraud prevention, Know your Customer (KYC) and Anti Money Laundering (AML) regulatory efforts by automating the workflow. With single API integration, Shufti Pro empowers you to verify customers with document checks from 3000+ ID templates and business entities from 200 million companies data.

Disclaimer: No warranty or claim is herein provided that information contained in this document is accurate, up-to-date, and/or complete. All information provided in this document is limited for general informational purposes only. In no circumstance(s), does such information constitute as legal or any other advice. Any individual or company who intends to use, rely, pass-on, or re-publish the information contained herein in any way is solely responsible for the same and any likely outcomes. Any individual or company may verify the information and/or obtain expert advice independently if required.