



THE UTILISATION OF HOME AFFAIRS DATA BY BANKS IN SOUTH AFRICA: BALANCING DATA PRIVACY, SECURITY, AND COMPLIANCE

By

Ntombiyenhlanhla Thabede

Submitted in partial fulfilment of the requirements for the degree of
Master of Laws by Coursework and Research Report
at the University of the Witwatersrand, Johannesburg

Supervisor

Professor Victoria Bronstein

Date: 24 March 2025

DECLARATION

I declare that this report is my own, unaided work. It is submitted in partial fulfilment of the requirements for the degree of Master of Laws in the field of Privacy Law at the University of the Witwatersrand, Johannesburg. It has not been submitted before for any other degree or examination in any other university.

1508299
<STUDENT NUMBER>

Word count: 10133

1. ABSTRACT

This paper examines the utilisation of biometric data from the Department of Home Affairs National Identification System ('HANIS') by South African banks, focusing on balancing data privacy, security, and regulatory compliance. While HANIS has significantly improved identity verification and fraud prevention, its scope is deliberately limited to South African citizens and permanent residents, excluding non-citizens. This exclusivity poses challenges to broader financial inclusivity, particularly for undocumented populations, and reflects the complexities of expanding such systems. Additionally, HANIS faces substantial risks from outdated infrastructure and centralised data storage, which increase vulnerability to breaches. Drawing comparisons with advanced systems like Onfido, a UK-based identity verification platform, this study explores opportunities for modernisation through decentralised models, artificial intelligence ('AI'), and blockchain technology, while emphasising the importance of safeguards to address errors in automated systems. In contrast, case studies on breaches in India's Aadhaar and Nigeria's Bank Verification Number ('BVN') systems highlight vulnerabilities common to centralised databases, emphasising the critical need for robust encryption, multi-factor authentication ('MFA'), and accessible error resolution mechanisms to protect user rights. Recommendations include adopting regulatory sandboxes to promote innovation, implementing advanced security measures, and improving inclusivity for underserved communities already within HANIS's scope. By addressing these challenges, South Africa can develop a secure, modernised framework that strengthens identity verification, fosters public trust, and enhances financial inclusion while safeguarding sensitive data.

Table of Contents

1. ABSTRACT	3
2. LIST OF ACRONYMS	5
3. INTRODUCTION	6
4. THE ROLE OF BIOMETRIC AUTHENTICATION IN BANKING	7
a) <i>Challenges in biometric adoption</i>	9
5. BIOMETRIC SYSTEMS IN SOUTH AFRICA – HANIS AND ITS INTEGRATION	11
6. COMPARATIVE CASE STUDY - HANIS AND ONFIDO	13
a) <i>Similarities and differences between HANIS and Onfido</i>	15
b) <i>Lessons for HANIS from Onfido and the ICO Regulatory Sandbox</i>	16
c) <i>AI and machine learning in identity verification</i>	17
d) <i>Data flow and regulatory compliance</i>	19
e) <i>Costs and complexities of regulatory sandboxes</i>	19
f) <i>Decentralised vs. centralised approaches</i>	20
g) <i>Managing risks in biometric authentication for banks</i>	21
7. CASE STUDIES	22
a) <i>The Aadhaar breach incident</i>	22
b) <i>The BVN security breach incident</i>	25
8. TECHNOLOGICAL ADVANCEMENTS	26
a) <i>Encryption and blockchain integration</i>	27
b) <i>Technological advancements in AI-driven biometric systems</i>	28
c) <i>Addressing fairness and inclusivity</i>	30
9. CONCLUSION	31
10. BIBLIOGRAPHY	34

2. LIST OF ACRONYMS

1. **AES:** Advanced Encryption Standard
2. **AI:** Artificial Intelligence
3. **ATM:** Automated Teller Machine
4. **BVN:** Bank Verification Number
5. **CA:** Continuous Authentication
6. **CBN:** Central Bank of Nigeria
7. **DHA:** Department of Home Affairs
8. **DPIA:** Data Protection Impact Assessment
9. **EEA:** European Economic Area
10. **FCA:** Financial Conduct Authority
11. **GDPR:** General Data Protection Regulation (EU)
12. **HANIS:** Home Affairs National Identification System
13. **ICO:** Information Commissioner's Office (UK)
14. **MFA:** Multi-Factor Authentication
15. **NIBSS:** Nigeria Inter-Bank Settlement System
16. **NINs:** National Identity Numbers
17. **PIN:** Personal Identity Number
18. **POPIA:** Protection of Personal Information Act
19. **SABRIC:** South African Banking Risk Information Centre
20. **SASSA:** South African Social Security Agency
21. **SMEs:** Small and Medium Enterprises
22. **UIDAI:** Unique Identification Authority of India

3. INTRODUCTION

The rapid global rise in cybercrime, identity theft, and financial fraud has placed immense pressure on the financial sector to adopt more secure and reliable identity verification methods. Traditional approaches – such as passwords, PINs, and security tokens – are increasingly vulnerable to breaches, prompting financial institutions to search for solutions that balance enhanced security with user convenience. Biometric authentication has emerged as a cutting-edge solution by leveraging “unique biological traits or behavioural characteristics, such as fingerprints or facial recognition”¹, to enhance security and improve user experiences. “Unlike traditional credentials, biometric identifiers are inherently tied to individuals and offer higher levels of accuracy, though they introduce long-term risks if compromised.”²

In South Africa, the HANIS has become a critical part of the banking sector’s identity verification process. By connecting financial institutions to the Department of Home Affairs (‘DHA’) database, HANIS “facilitates real-time identity verification”³, reduces fraud, and ensures compliance with Know Your Customer (KYC) regulations. This system “fosters trust and operational efficiency”⁴, but its limitations pose challenges to broader financial inclusion and security.

A key limitation of HANIS is its exclusion of non-citizens, including undocumented residents and refugees, reflecting its primary role of protecting national identity and serving South African citizens and permanent residents. However, within its mandate, HANIS still faces challenges in promoting inclusion for underserved citizens, such as those in rural areas with limited access to formal financial services due to logistical, economic, and infrastructural barriers.⁵ Addressing these disparities is crucial for ensuring equitable access to financial services. For non-citizens, banks already rely on alternative verification systems to facilitate access, highlighting the need for a complementary approach between HANIS and external systems.

¹ M Balamurugan ‘Biometric Authentication: A Double-Edged Sword for Security?’ (2023) *IJSR* 170.

² Balamurugan op cit note 1.

³ South African Government ‘Verify identity online’ available at <https://www.gov.za> accessed on 28 March 2024.

⁴ SABRIC ‘Department of Home Affairs (DHA) Online Services’ available at <https://www.sabric.co.za> accessed on 28 March 2024.

⁵ Berverly Chauke Migrants and access to financial services: exploring alternative financial services available to Zimbabwean migrants who have no access to formal financial services in South Africa (Unpublished master's thesis, University of Pretoria, 2020) 4.

Another challenge is HANIS's reliance on outdated infrastructure⁶, which cannot keep pace with South Africa's growing digital banking sector. Legacy systems are prone to inefficiencies, technical failures, and vulnerabilities to cyberattacks. The centralised nature of its databases further exacerbates these risks, as breaches could compromise large volumes of sensitive biometric data. "Centralised systems store data in a single location, making them efficient but vulnerable to breaches if not properly protected."⁷

Lessons from the UK Onfido's advanced biometric system and the data breaches in Aadhaar and BVN provide valuable insights. Onfido's use of AI and decentralised data storage "offers enhanced security by minimising reliance on a central authority"⁸, thereby "reducing risks of data tampering and unauthorised access"⁹. Meanwhile, Aadhaar and BVN highlight the dangers of centralised databases and underscore the importance of robust encryption, multi-factor authentication (MFA), and user-friendly mechanisms for resolving errors.

This paper examines HANIS's role in South Africa's banking sector, analysing its strengths and limitations within the context of global best practices. It explores how emerging technologies like AI, machine learning, blockchain, and advanced encryption can help modernise the system and align it with international standards. By addressing systemic gaps, such as inclusion challenges within its scope and cybersecurity vulnerabilities, South Africa can build a secure and future-ready biometric framework that supports its growing financial ecosystem.

4. THE ROLE OF BIOMETRIC AUTHENTICATION IN BANKING

The adoption of biometric authentication in the banking sector in South Africa presents numerous benefits that enhance security, improve customer experience, and comply with regulatory requirements. Biometric authentication operates by comparing the "biometric features of an individual with those stored in a database, and only when a match is found is

⁶ Department of Home Affairs 'Strategic plan' available at <https://www.dha.gov.za> accessed on 26 March 2024.

⁷ A Mohammed & BM Saleh 'Centralized database: A prerequisite for security and sustainable development in Nigeria' (2017) *IJIRCST* 209.

⁸ S Islam & KU Apu 'Decentralized vs. centralized database solutions in blockchain: advantages, challenges, and use cases' (2024) 3(4) *Global Mainstream Journal of Innovation* 58.

⁹ Islam & Apu op cit note 8.

access granted.”¹⁰ This technology is increasingly recognised as a robust alternative to traditional password-based systems, which are often vulnerable to breaches and fraud. In contrast, biometric identifiers “are unique to each individual and cannot be easily replicated, misplaced or forgotten”.¹¹ Furthermore, the use of biometric systems can reduce the risk of unauthorised access, thereby bolstering the overall security framework of banking institutions.

In addition to security improvements, biometric authentication enhances customer trust and improves brand reputation. As customers become increasingly aware of the risks associated with online banking, the implementation of reliable biometric systems can foster greater confidence in financial institutions.¹² Research indicates that customers perceive biometric technologies as more secure compared to traditional methods, which can lead to increased usage and loyalty towards banks that adopt such technologies.¹³ Moreover, the convenience offered by biometric systems, eliminating the need for remembering complex passwords, can significantly enhance user experience, making banking services more accessible and user-friendly.¹⁴

Regulatory compliance is another critical aspect driving the adoption of biometric authentication in banks. With increasing legislative requirements for multi-factor authentication, banks are compelled to implement more secure methods to protect sensitive customer data.¹⁵ Biometric systems not only meet these regulatory demands but also provide a competitive edge in the market by showcasing a commitment to security and innovation.¹⁶

The scalability and flexibility of biometric solutions make them highly adaptable for various banking applications, ranging from ATM transactions to mobile banking. Scalability in this context refers to the ability of biometric systems to handle increasing volumes of users or

¹⁰ A Bodepudi & M Reddy ‘Cloud-Based Biometric Authentication Techniques for Secure Financial Transactions: A Review’ (2020) 4(1) *International Journal of Information and Cybersecurity* 2.

¹¹ A Gelb & J Clark ‘Identification for development: The biometrics revolution’ (2013) 315 *Center for Global Development Working Paper* 62.

¹² S Tatineni ‘Customer authentication in mobile banking—mlops practices and AI-driven biometric authentication systems’ (2022) 3.4 *Journal of Economics & Management Research* 1.

¹³ A Morake, L Khoza & T Bokaba ‘Biometric technology in banking institutions: the customers’ perspectives’ (2021) 23 *SAJIM* 2-3.

¹⁴ K Prihodova & M Hub ‘Hand-based biometric system using convolutional neural networks’ (2020) 9(1) *Acta Informatica Pragensia* 49.

¹⁵ Prihodova & Hub op cit note 13.

¹⁶ D Laux *et al* ‘Adoption of biometric authentication systems: implications for research and practice in the deployment of end-user security systems’ (2011) 21(3) *JOCEC* 221-223.

transactions without compromising performance or security. This means banks can expand their use of biometric authentication as their customer base grows or as transaction demands increase, ensuring the technology remains effective and reliable at larger scales. Moreover, the ability to integrate biometric authentication seamlessly into existing systems allows banks to enhance security without the need for a complete infrastructure overhaul.¹⁷ This adaptability is particularly valuable in a rapidly evolving digital landscape, where cyber threats are becoming more sophisticated and banks must continually improve their defences to stay ahead.

The benefits of using biometric authentication in South African banks are multifaceted, encompassing enhanced security, improved customer experience, regulatory compliance, and operational flexibility. As the banking sector continues to evolve, the integration of biometric technologies will likely play a pivotal role in shaping the future of secure financial transactions.

a) Challenges in biometric adoption

Despite their advantages, biometric systems face challenges related to inclusivity. Barriers such as lack of access to technology, literacy issues, and physical disabilities disproportionately affect marginalised groups, thus limiting their participation in the formal banking sector.

“Poor people, rural residents, and elderly people face logistical and travel challenges when seeking identity credentials. The direct and indirect costs associated with obtaining or using these credentials, such as application fees, travel expenses, and lost wages, can be prohibitively high for them. Additionally, many don't have access to smartphones or other resources necessary for engaging with online or digital services. The elderly people often struggle to provide biometrics and may have limited access to, or literacy in using digital services. Similarly, persons with disabilities may face mobility challenges or have no access to centres that accommodate their needs, which can hinder their registration process. Furthermore, the DHA may not have adequately trained staff or inclusive enrolment procedures. People with lower literacy levels also face difficulties, particularly since application forms are typically written in English or Afrikaans, making it challenging for them to complete the necessary paperwork.”¹⁸

The South African Social Security Agency (‘SASSA’) offers an illustrative example of these challenges in the context of social grant distribution. SASSA’s biometric system, designed to

¹⁷ Panini ‘The future of biometric authentication in banking’ available at <https://www.panini.com> accessed on 29 July 2024.

¹⁸ Department of Home Affairs ‘Draft Official Identity Management Policy (Public Consultation Version)’ available at <http://www.dha.gov.za> accessed on 30 July 2024.

combat fraud and improve efficiency, highlights the difficulties faced by marginalised populations.¹⁹ While the system has reduced fraudulent claims and streamlined grant payments, it has also exposed critical accessibility issues. Beneficiaries in remote areas often lack the necessary infrastructure, such as internet connectivity, to complete biometric verifications. The biometric verification process requires infrastructure that may be difficult to implement in areas where internet access or biometric registration points are limited. This technological gap may prevent some eligible beneficiaries from receiving grants.²⁰ In some cases, legitimate beneficiaries may experience difficulties verifying their identity due to issues such as worn-out fingerprints, which is particularly common in older individuals.²¹ “The false rejection error occurs when the authentication device is unable to identify the person and rejects the authentication process.”²² These false rejections can cause delays and frustration, potentially preventing those who need the funds most from receiving them. These experiences underline the importance of designing systems that prioritise accessibility and inclusivity, ensuring equitable access for all.

In South Africa, the adoption of biometric systems is further hindered by outdated infrastructure and resource constraints. Many systems rely on legacy technologies that lack the capacity to handle modern demands efficiently. This results in slower authentication processes, increased maintenance costs, and greater susceptibility to technical failures. Upgrading infrastructure to support advanced biometric systems is critical to overcoming these limitations and ensuring broader access.

Centralised biometric systems, such as HANIS, introduce significant security risks due to their reliance on single points of failure. These systems are attractive targets for cyberattacks, as breaches can compromise vast amounts of sensitive data. For instance, the Aadhaar breach in India demonstrated the devastating consequences of inadequate security measures in centralised databases. A cyber incident can severely disrupt a financial institution's ability to function, leading to substantial financial losses and operational failures. This is particularly

¹⁹ Status Check ‘SASSA Implements Biometric Verification to Combat Fraud’ available at <https://statuscheck.co.za> accessed on 29 November 2024.

²⁰ Institute for Economic Justice ‘UBIC Statement | Government needs to urgently clarify its policies on the SRD Grant, the social grant system, and Basic Income’ available at <https://iej.org.za> accessed on 28 December 2024.

²¹ Status Check op cit note 18.

²² Barkat Hussaini Risks and challenges associated with Biometric authentication in multifactor authentication systems (Thesis, Jonkoping University School of Engineering 2024) 13.

concerning in the context of the interconnectedness of financial systems, where a breach in one institution can jeopardise the solvency of others due to shared dependencies and trust networks.²³

Furthermore, the reputational risk that arises from such incidents can erode customer trust, which is crucial for the sustainability of financial services.²⁴ Operational risks, including system downtime and technical glitches, further amplify these vulnerabilities, potentially disrupting banking services

5. BIOMETRIC SYSTEMS IN SOUTH AFRICA – HANIS AND ITS INTEGRATION

The integration of biometric systems into South Africa's banking sector has been significantly advanced through HANIS, managed by the DHA, in collaboration with the South African Banking Risk Information Centre ('SABRIC'). "HANIS is a computerised database storing personal information and biometric data of South African citizens and permanent residents."²⁵ It enables real-time identity verification, ensuring compliance with KYC regulations, preventing fraud, and enhancing banking efficiency.²⁶ SABRIC, an industry body combating organised crime and fraud, supports this integration by providing risk mitigation strategies, intelligence, and promoting collaboration within the financial services sector.²⁷ Together, these initiatives have created a secure and efficient banking environment by leveraging advanced biometric systems to mitigate risks and improve service delivery.

South African banks use HANIS to verify customer identities in real time via a secure Application Programming Interface ('API'). The API serves as a bridge between banks and the DHA, enabling seamless data exchange.

"APIs are considered a secure way of giving third-party providers access to customers' financial information to enable the provision of enhanced services, as they do not involve sharing sensitive information like login credentials. This should, however, involve banks

²³ U Islam et al 'Detection of distributed denial of service (ddos) attacks in IoT-based monitoring system of the banking sector using machine learning models' (2022) 14(14) *Sustainability* 1.

²⁴ OE Akinbowale et al The assessment of the impact of cyberfraud in the South African banking industry (Thesis, Tshwane University of Technology, 2023) 292.

²⁵ Temitope Lawal 'HANIS online verification: FAQ on HANIS verification services' available at <https://youverify.co> accessed on 24 March 2024.

²⁶ Jacob Nthoiwa 'Banks to access Home Affairs data' available at <https://www.itweb.co.za> accessed on 20 May 2024.

²⁷ SABRIC op cit note 4.

getting permission from their customers to share certain of their account information with third-party APIs in a secure and seamless manner.”²⁸

When a client visits a bank branch, they provide their thumbprint for biometric authentication. This thumbprint is scanned and transmitted to the DHA database via the secure API. “The fingerprint presented is then compared to the stored fingerprint.”²⁹ The system then retrieves vital client information such as name, surname, ID number, marital status and, in some cases, a client’s image. This real-time data exchange significantly enhances the speed and accuracy of identity verification, reducing the time needed for onboarding new clients and detecting potential fraud. It is particularly beneficial for online banking services, where traditional verification methods may be cumbersome or less secure.

For banks that operate without physical branches, the authentication process is similarly streamlined. They use the secure API to log in to the DHA system. By entering the client’s ID number, the system pings DHA and retrieves the same set of client details. This capability is particularly beneficial for online banking services, where traditional methods of verification may be cumbersome or inadequate. The reliance on biometric data and direct access to government databases represents a paradigm shift in client verification, as banks increasingly adopt a technology-driven model while ensuring strong security standards. The security of the API connection is paramount, as it protects sensitive personal information from unauthorised access.³⁰ The system uses encryption, secure access protocols, and strict permissions to ensure the confidentiality and integrity of data transmitted between banks and the DHA. These measures reduce the risk of data breaches associated with shared networks and foster trust by ensuring compliance with regulatory requirements.

The API connection is designed with robust security measures, including encryption and strict access protocols, to ensure the confidentiality and integrity of data transmitted between banks and the DHA. These safeguards protect sensitive client information from unauthorised access, minimise the risk of data breaches associated with shared or unsecured networks, and ensure compliance with data protection regulations, fostering client trust.

²⁸ South African Reserve Bank ‘Consultation paper on open-banking activities in the national payment system’ (2020) *National Payment System Department* 13.

²⁹ Lawal op cit note 24.

³⁰ Wiz ‘What is API security’ available at <https://www.wiz.io> accessed on 29 December 2024.

The implications of this integration extend beyond mere efficiency; they also encompass broader societal benefits. By improving the accuracy and speed of identity verification, banks can better serve their clients, particularly those who may have previously faced barriers to accessing financial services. This is particularly relevant in the context of financial inclusion, where marginalised populations often struggle to provide the necessary documentation for banking services. The ability to authenticate identities through biometric data and direct government access can help bridge this gap, allowing more individuals to participate in the formal banking system.³¹ In addition to enhancing client service, this integration aligns with global trends in secure digital identity management. As financial institutions increasingly migrate operations online, mechanisms like HANIS and SABRIC's API integration set a benchmark for leveraging technology to create a safer, more inclusive banking system.

6. COMPARATIVE CASE STUDY - HANIS AND ONFIDO

Onfido is an identity verification platform that leverages advanced technologies to provide secure and scalable solutions. Its approach centres on integrating AI and machine learning to enhance identity verification processes. By utilising cutting-edge algorithms, Onfido can verify the authenticity of documents and match biometric data in real-time, reducing the risk of identity fraud.

When banks integrate with Onfido, the data flow typically involves collecting personal information, such as identification documents, biometric data, and other relevant details from users. Onfido processes this information and supplements it with data from trusted third-party providers to validate user identities. This multi-source approach enhances the accuracy and reliability of identity verification, crucial in the banking sector to mitigate financial risks associated with fraud. Additionally, Onfido's biometric checks allow users to submit a selfie and an image of their identity document. The platform generates two scans, one from the selfie and one from the reference image, and compares them to verify the person's identity.

“When providing biometric checks as part of its Identity Services, Onfido will ask for an image or video (including an audio recording) of a user's face (a “Selfie”), as well as an image or

³¹ UI Nnaomah et al ‘Digital banking and financial inclusion: a review of practices in the USA and Nigeria’ (2024) 6(3) *Finance & Accounting Research Journal* 465.

video to use as a reference image (for example, an image of their identity document). It then generates two scans of the user's face (one from the Selfie, and one from the reference image) and compares those two scans to assess whether the person in the Selfie is likely to be the same person pictured in the reference image.”³²

Onfido can also help clients to determine whether a device, email address or phone number has previously been used in relation to suspected fraudulent activity; shows unusual usage patterns that have been manipulated; or otherwise indicates that the user may not be genuine.³³

The integration of Onfido's technology into banking operations improves user experience while fortifying security measures against fraud. It allows banks to comply with regulatory standards while ensuring the transparency and accuracy of user data.

“The information collected will vary depending on the availability of checks in the user's location and the Identity Services selected by Onfido's clients. It may include contact details such as postal address, email address, telephone number, social security number or other national identity number, information extracted from a utility bill a user uploads or other information provided by the Data Provider e.g. a user's mobile network operator, publicly available information from media searches, sanctions and PEP lists.”³⁴

Onfido operates as both a service provider and a data controller. While processing personal information on behalf of clients, it also uses aggregated data to improve its identity verification technologies to develop and improve its Identity Services.³⁵ This dual role highlights the importance of maintaining data integrity, as banks must provide accurate information to ensure compliance with privacy regulations such as the General Data Protection Regulation (‘GDPR’) in the UK and the European Economic Area (‘EEA’). In terms of regulatory compliance, particularly in the EEA and the UK, banks are responsible for identifying the legal basis for processing personal information.³⁶ Transparency in data usage is essential for building trust and adhering to legal obligations.

The Information Commissioner's Office (‘ICO’) emphasises fairness and inclusivity in biometric verification technologies. Organisations like Onfido must rigorously assess their systems to mitigate biases and avoid discrimination based on race, gender, or other

³² Onfido ‘Onfido Privacy Policy’ available at <https://onfido.com> accessed on 30 July 2024.

³³ Onfido op cit note 31.

³⁴ Ibid at 32.

³⁵ Ibid at 32.

³⁶ Ibid at 32.

characteristics. Transparency in processing biometric data is critical to maintaining user trust and regulatory compliance.

a) Similarities and differences between HANIS and Onfido

Both HANIS and Onfido use advanced technologies to facilitate identity verification processes, focusing on automation, fraud prevention, and operational efficiency. Onfido use AI and machine learning algorithms to analyse identity documents and biometric data, ensuring accuracy and security in identity verification.³⁷ The company's platform is designed to streamline the onboarding process for businesses by providing real-time verification services, which is crucial in sectors such as finance and e-commerce where regulatory compliance is paramount.³⁸ Similarly, HANIS also leverages AI to enhance its identity verification solutions, focusing on automating the verification process to reduce manual intervention and improve efficiency. This shared reliance on AI underscores a common trend in the industry towards automation and enhanced security measures. Onfido and HANIS aim to streamline processes, reduce manual intervention, and bolster security against identity fraud.

However, differences between the platforms are significant. Onfido has established itself as a leader in the identity verification market, particularly in the UK and Europe, and has a broader range of services that include document verification, facial recognition, and background checks.³⁹ Onfido's remote biometric identity verification technology is similar to the more traditional act of proving identity in person.⁴⁰ Its extensive experience and partnerships with various industries, including banking and healthcare, allow it to offer tailored solutions that meet specific regulatory requirements. In contrast, HANIS appears more focused on a specific sector (banks) with potentially limited scalability.

This difference in market focus may influence the scalability and adaptability of their services, with Onfido being better positioned to handle large-scale operations due to its established infrastructure and client base. Furthermore, the user experience and integration capabilities of both platforms differ. Onfido provides a robust API that allows businesses to easily integrate

³⁷ Lubna Takruri 'How to verify ID easily: a comprehensive guide' available at <https://onfido.com> accessed on 24 March 2024.

³⁸ Easydebit 'Client onboarding compliance: navigating regulatory challenges with ease' available at <https://www.easydebit.co.za> accessed on 26 March 2024.

³⁹ Paul Jarratt 'Onfido named as a market leader in kuppingercole's 2022 market compass: providers of verified identity' available at <https://onfido.com> accessed on 30 July 2024.

⁴⁰ Onfido 'Regulatory Sandbox Final Report: Onfido' available at <https://ico.org.uk> accessed on 30 July 2024.

its verification services into their existing systems, enhancing user experience and operational efficiency.⁴¹ This flexibility is crucial for companies looking to maintain a seamless customer journey while ensuring compliance with identity verification regulations. HANIS, while also offering integration options, may not have the same level of API sophistication or market penetration, which could limit its appeal to larger enterprises seeking comprehensive solutions.

b) Lessons for HANIS from Onfido and the ICO Regulatory Sandbox

The centralised design of HANIS, while enabling real-time identity verification, poses significant security risks. Centralised systems are particularly appealing to cybercriminals due to their single point of failure; a successful breach can compromise all stored data. The Aadhaar breach in India serves as a cautionary tale, illustrating how inadequate encryption and weak authentication measures can threaten the integrity of centralised systems.

To address these vulnerabilities, HANIS could adopt a decentralised model similar to Onfido's, which distributes data storage across multiple nodes. This approach reduces risks, ensuring that even if one node is compromised, the overall system remains secure. Additionally, implementing advanced encryption methods, multi-factor authentication (MFA), and continuous monitoring can further protect data integrity.

HANIS can also leverage AI-driven solutions to enhance scalability and decrease costs traditionally linked to manual processes. By incorporating advanced biometric techniques, such as facial recognition, HANIS could significantly improve both accuracy and security.

To support such advancements, South Africa could introduce a regulatory sandbox, modelled after the ICO's framework, to encourage innovation while ensuring robust data protection standards. A regulatory sandbox creates a collaborative environment "where regulators and private sector entities can test and refine new services under controlled conditions".⁴² This approach provides valuable insights into the practical application of emerging technologies.

⁴¹ Takruri op cit note 36.

⁴² Sofia Ranchordas 'Experimental regulations for AI: sandboxes for morals and mores' (Research Paper 7 thesis, University of Groningen Faculty of Law, 2021) 13.

Adopting a sandbox framework would empower HANIS to “pilot innovative technologies”⁴³, ensure compliance with regulations, and “reduce time-to-market by streamlining the authorisation process”.⁴⁴ It would also mitigate regulatory uncertainty by clarifying how the Protection of Personal Information Act No 4, of 2013 (‘POPIA’) applies to AI-driven solutions.⁴⁵

Furthermore, the sandbox model could “remove market-entry barriers for innovative companies, particularly small and medium enterprises (SMEs), while democratising access to legal and regulatory knowledge surrounding biometric technology”.⁴⁶ This would enable HANIS to innovate responsibly while maintaining alignment with user rights and data protection requirements.

By adopting a hybrid model that combines centralised oversight with decentralised data storage, HANIS can retain the benefits of a centralised system while mitigating its associated risks. Securely distributing sensitive data and integrating blockchain for tamper-proof audit trails, HANIS would enhance trust, transparency, and resilience against breaches.

c) AI and machine learning in identity verification

Onfido’s use of AI and machine learning for real-time identity verification offers a compelling advantage in fraud prevention. By comparing user selfies with government-issued IDs, Onfido enhances accuracy and minimises the risk of identity theft.⁴⁷ This model could serve as a blueprint for HANIS, which could adopt similar AI-driven solutions to improve scalability and reduce the costs associated with manual verification processes. However, while AI holds significant promise, over-reliance on automated systems introduces potential risks such as algorithmic bias, inaccuracies, and system failures. Bias refers to the systematic errors that occur in decision-making processes, leading to unfair outcomes.⁴⁸

⁴³ OECD ‘Regulatory sandboxes in artificial intelligence’ available at <https://www.oecd.org> accessed on 27 November 2024.

⁴⁴ OECD op cit note 42.

⁴⁵ Ibid at 43.

⁴⁶ Ibid at 43.

⁴⁷ Charlotte Bowyer ‘Electronic identity verification (eIDV)—what businesses need to know’ available at <https://onfido.com/blog> accessed on 25 August 2024.

⁴⁸ E Ferrara ‘Fairness and bias in artificial intelligence: A brief survey of sources, impacts, and mitigation strategies’ (2023) 6 *Sci* 2.

AI systems are only as effective as the data used to train them. Bias in datasets or inadequate diversity during system training can lead to unequal outcomes, particularly for marginalised groups. For example, studies have shown that AI-based facial recognition systems often exhibit higher error rates when identifying individuals from underrepresented demographics.⁴⁹ HANIS can prioritise equity by ensuring that its AI models are trained on diverse and representative datasets to reduce systemic bias and promote fairness.

Another critical consideration is error resolution. Users who are wrongly flagged by automated systems, whether due to inaccuracies or technical errors, must have accessible avenues to challenge these decisions. Both Section 71 of POPIA and Article 22 of the GDPR mandate “the right to meaningful human oversight in automated decision-making processes”⁵⁰. Given HANIS’s API-based integration, this oversight should be implemented at the institutional level. Banks and other entities using the HANIS API must offer user-friendly mechanisms for resolving disputes, allowing users to correct errors efficiently. Institutions should provide human support where necessary, guiding users in rectifying incorrect data, such as updating their biometric or personal details through the appropriate channels at DHA. This ensures compliance with regulatory requirements while preserving public trust and accountability.

Integrating advanced biometric authentication methods highlights the need to secure electronic signatures and biometric data with robust safeguards such as encryption and blockchain. These technologies align seamlessly with HANIS’s operational objectives, strengthening security and scalability while maintaining compliance with evolving regulations. Regulatory sandbox frameworks can further enable South Africa to refine AI-driven systems by testing innovative technologies in controlled environments, ensuring that security, compliance, and inclusivity are prioritised.

International experiences demonstrate how AI-powered biometric verification can enhance security and mitigate fraud in banking⁵¹, but only when paired with safeguards for ethical and inclusive implementation. A balanced approach, combining technological innovation with

⁴⁹ Rachel Fergus ‘Facial recognition remains largely ungoverned and dangerous in Minnesota’ available at <https://www.aclu-mn.org> accessed on 25 August 2024.

⁵⁰ Article 22 of the Regulation (EU) 2016/679 (GDPR).

⁵¹ A Gautam ‘The evaluating the impact of artificial intelligence on risk management and fraud detection in the banking sector’ (2023) 13 *AI, IoT and the Fourth Industrial Revolution Review* 11.

mechanisms for transparency, fairness, and accountability, will position HANIS to leverage AI effectively while avoiding common pitfalls.

d) Data flow and regulatory compliance

The ICO Regulatory Sandbox exemplifies a regulatory framework that allows for the testing of innovative technologies while ensuring compliance with GDPR. This model supports the “innovation of organisations working with emerging technologies, helps them prevent such harms to people’s privacy”.⁵² POPIA, while a step in the right direction, could benefit from a similar sandbox approach to enhance its regulatory framework.

Through such a sandbox, regulators could better “inform long-term policymaking by learning from industry experiments”⁵³ and fostering communication with market participants. From the consumer perspective, the sandbox could “promote the introduction of safer products”⁵⁴, ensuring user protection while “providing access to more innovative financial products and services”.⁵⁵

The principles outlined in POPIA, such as “accountability, processing limitation, purpose specification, and data subject participation”,⁵⁶ are essential for the lawful processing of personal information. These could be further strengthened through a sandbox model that encourages innovation while safeguarding user rights. Therefore, HANIS could adopt a sandbox-like framework to pilot its biometric solutions, ensuring compliance while fostering innovation.

e) Costs and complexities of regulatory sandboxes

While regulatory sandboxes offer significant benefits, “establishing one is complex and costly”.⁵⁷ It requires substantial investment in hiring experienced regulators to work closely with fintech companies over extended periods.⁵⁸ For instance, the UK Financial Conduct

⁵² ICO ‘Our current areas of focus for the Regulatory Sandbox’ available at <https://ico.org.uk> accessed on 30 July 2024.

⁵³ Ibid at 43.

⁵⁴ Ibid at 43.

⁵⁵ Ibid at 43.

⁵⁶ R Adams et al ‘Drafting a Code of Conduct for research under the Protection of Personal Information Act No. 4 of 2013’ (2021) 117 *SAJS* 1.

⁵⁷ E Brown & D Piroška ‘Governing fintech and fintech as governance: The regulatory sandbox, risk washing, and disruptive social classification’ (2022) 27 *New Political Economy* 4.

⁵⁸ Brown & Piroška op cit note 56.

Authority ('FCA') leveraged significant financial resources to build a successful sandbox within a rich fintech ecosystem.⁵⁹ South Africa, with more limited resources, may face challenges in replicating this success without external support or strategic prioritisation.

To overcome these challenges, HANIS could partner with private sector stakeholders to share financial burdens, leverage international expertise for guidance, and phase the implementation to manage costs incrementally. This approach would allow HANIS to develop the necessary infrastructure and regulatory framework gradually while maintaining a focus on innovation and compliance.

f) Decentralised vs. centralised approaches

Onfido's decentralised model allows for cross-border identity verification⁶⁰, making it particularly advantageous for global financial institutions. In contrast, HANIS's current limitation to South African citizens reflects its primary purpose of serving domestic identification needs. While this limitation aligns with national security and governance priorities, it restricts HANIS's ability to support cross-border financial transactions and the verification of non-citizens. However, focusing on modernising HANIS within its domestic context can still deliver significant benefits for financial inclusion and regulatory compliance.

By adopting a more decentralised approach and leveraging a sandbox framework, HANIS can enhance its internal efficiency and security while aligning with evolving legal standards under POPIA. Early engagement with regulators through sandbox testing⁶¹ would allow HANIS to experiment with emerging technologies like blockchain and advanced encryption in a controlled environment, mitigating risks and ensuring compliance before full-scale implementation.

Expanding internationally is currently beyond HANIS's mandate. However, improvements to its core infrastructure, such as decentralised data storage and robust biometric verification, could still provide indirect support to South African financial banks engaging in cross-border transactions. For example, secure and verified data from HANIS could help banks streamline

⁵⁹ G Cornelli et al 'Regulatory sandboxes and fintech funding: evidence from the UK' (2024) 28 *Review of Finance* 213.

⁶⁰ DcentAI 'Decentralized AI for digital identity verification' available at <https://medium.com> accessed on 29 December 2024.

⁶¹ Ibid at 43.

compliance with KYC requirements when offering cross-border financial services to South African citizens.

Stakeholder insights into biometric data protection highlight the importance of balancing innovation with regulatory compliance and user rights. By integrating advanced security protocols and adopting collaborative regulatory strategies, HANIS can foster trust within South Africa's financial ecosystem while serving as a model for secure, citizen-focused biometric systems.

g) Managing risks in biometric authentication for banks

Managing the risks associated with biometric authentication requires a thorough understanding of technological capabilities and vulnerabilities. Banks adopting such technologies should implement robust strategies to address risks like data breaches, identity theft, and unauthorised access. One effective strategy is the implementation of multi-factor authentication ('MFA'). MFA enhances security by "combining two or more independent credentials to verify a user's identity"⁶². These credentials typically include: "what the user knows, such as a password; what the user possesses, such as a security token; and what the user inherently is, verified through biometric methods"⁶³ like fingerprints or facial recognition.

MFA adds additional layers of verification and mitigates risks associated with single biometric modalities. Continuous authentication ('CA') frameworks, which monitor user behaviour throughout banking transactions, further strengthen security. "CA systems are an additional security measure that monitor users' biometric behaviour by constantly re-authenticating them during a login session."⁶⁴ For example, touch dynamics biometrics, which analyse how users interact with their devices, ensure ongoing verification without disrupting the user experience, reducing the likelihood of fraud.

Data protection is equally critical. Encrypting biometric templates and storing them in non-reversible formats safeguards sensitive data. This ensures that even if attackers gain access to the data, it cannot be reconstructed. Educating users about the importance of biometric security also fosters trust, as informed users are more likely to adopt these technologies confidently.

⁶² Kinza Yasar 'What is multifactor authentication?' available at <https://www.techtarget.com> accessed on 29 November 2024.

⁶³ Yasar op cit note 61.

⁶⁴ Ioannis Stylios & Samos Aegean Behavioral biometrics for continuous authentication: security and privacy issues (Unpublished PhD thesis, University of the Aegean, Greece, 2023) 24.

Compliance with legislative frameworks governing biometric data usage is essential. Banks must adhere to best practices for data protection, not only to mitigate legal risks but also to enhance customer confidence in biometric systems.

By learning from Onfido's technology and the ICO Regulatory Sandbox, HANIS can leverage AI and machine learning for efficient identity verification, adopt regulatory sandbox frameworks to foster innovation while ensuring compliance, and transition to a decentralised model to improve scalability and promote financial inclusion. For banks, effective risk management strategies and adherence to regulatory frameworks are crucial for the secure implementation of biometric authentication technologies, which are critical to building trust and advancing user adoption.

7. CASE STUDIES

a) The Aadhaar breach incident

The Aadhaar breach in India highlights the critical risks associated with large-scale biometric data collection and centralised digital identity systems. Managed by the Unique Identification Authority of India (UIDAI), Aadhaar is one of the world's largest biometric databases, storing sensitive data such as fingerprints and iris scans for over a billion Indian residents.⁶⁵ Although Aadhaar was designed to improve access to services by issuing unique identification numbers, its security vulnerabilities have raised significant concerns about data protection and privacy. Similar to HANIS, Aadhaar relies on a centralised biometric database. While this design improves operational efficiency, it also introduces major risks.. Centralised databases are often criticised for their vulnerability to breaches.⁶⁶ "Persistent threats, such as unauthorised access and accidental data leaks due to technical flaws or human error"⁶⁷, highlight the dangers of centralisation and demonstrate the importance of robust safeguards.

"Biometric data, despite its advantages, is not immune to attacks. Vulnerabilities in biometric systems can compromise their integrity and security, leading to unauthorised access and misuse. Preventing these attacks requires robust security measures, continuous monitoring, and

⁶⁵ A Shweta et al 'Privacy and security of Aadhaar: a computer science perspective' (2017) *Economic and Political Weekly* 93.

⁶⁶ P Dixon 'A failure to "do no harm"--India's Aadhaar biometric ID program and its inability to protect privacy in relation to measures in Europe and the US' (2017) 7 *Health and Technology* 544.

⁶⁷ Dixon op cit note 65.

regular updates to biometric systems.”⁶⁸ However, Aadhaar’s rapid expansion outpaced the development of such safeguards, leaving the system exposed to security breaches and systemic vulnerabilities.

Introduced in 2009, Aadhaar assigns a 12-digit unique identification number to each Indian resident, linking it to both demographic and biometric information.⁶⁹ The system is widely used for identity verification across government services, banks, mobile connections, and welfare programs. Processing billions of transactions annually, it plays a critical role in everyday life. However, its rapid implementation without adequate privacy and security measures created vulnerabilities that eventually led to the 2018 breach.

The breach occurred when unauthorised access was gained through a portal managed by a state-owned utility company.⁷⁰ Sensitive information, including names, addresses, and Aadhaar numbers, was accessed without proper authentication. Reports also suggested that biometric data, such as fingerprints and iris scans, was at risk of misuse. The lack of adequate security measures, including insufficient encryption, made the system vulnerable to interception. Additionally, the absence of multi-factor authentication and role-based access controls allowed attackers to exploit system weaknesses. “These vulnerabilities enabled malicious actors to compromise sensitive personal data. Addressing such issues requires a complete overhaul of security protocols, the integration of advanced encryption technologies, and stricter access controls.”⁷¹

The failure of UIDAI’s monitoring mechanisms to detect and prevent the breach revealed major regulatory gaps and weak oversight. The breach had widespread consequences, significantly reducing public trust in the Aadhaar system. Many individuals feared identity theft and financial fraud, especially since Aadhaar was linked to essential services like bank accounts, mobile numbers, and welfare benefits. Businesses relying on Aadhaar for customer verification faced disruptions and incurred additional costs while seeking alternative methods. The incident

⁶⁸ D Sadhya & T Sahu ‘A critical survey of the security and privacy aspects of the Aadhaar framework’ (2024) 140 *Computers & Security* nil.

⁶⁹ I Pali et al ‘A comprehensive survey of Aadhaar and security issues’ (2020) *arXiv preprint arXiv:2007.09409* 1.

⁷⁰ Wolfe Systems ‘A closer look at the Aadhaar 2018 cybersecurity breach’ available at <https://wolfesystems.com.au> accessed on 19 June 2024.

⁷¹ Legal Service India ‘Understanding the Aadhaar Data Breach: Causes, Consequences, and Future Safeguards’ available at <https://legalserviceindia.com> accessed on 29 August 2024.

also exposed the risks of Aadhaar's rapid deployment. Deployed in less than a decade, the system's fast rollout left critical privacy safeguards either inadequate or missing, contributing to the scale and impact of the breach.

In response, India passed the Digital Personal Data Protection Act, 2023, to regulate how personal data is collected and processed.⁷² However, concerns remain. Critics argue that the law fails to address "surveillance oversight and lacks independent regulatory mechanisms".⁷³ As a result, millions of individuals may still be vulnerable to the misuse of their personal and biometric data. "UIDAI implemented several security upgrades, including encrypting biometric data"⁷⁴ including encrypting biometric data at the point of capture and enhancing system monitoring protocols. However, experts argue that these improvements must be supported by comprehensive and enforceable regulations to be effective. As one report emphasised, "UIDAI must build multi-factor authentication to build a secure application and also need to take care of session timeouts. UIDAI must also have enough provisions to secure the endpoint of the transactional layer."⁷⁵ Furthermore, India lacks "a nation-wide encryption policy to regulate data security"⁷⁶, and "several applications don't ensure end-to-end encryption for users' personal information,"⁷⁷ leaving key gaps in protection.

Stronger regulatory oversight is essential to ensuring that institutions comply with security requirements and take swift action in the event of future breaches. The Aadhaar breach serves as a cautionary tale, highlighting the need for robust security measures, regulatory vigilance, and effective data management practices. Centralised biometric databases like Aadhaar pose inherent risks due to the sensitive nature of the data they store. Without proper legal frameworks, oversight mechanisms, and technological safeguards, these systems are prone to breaches that can undermine public trust. Moving forward, India must address these issues by closing legal loopholes and enforcing stronger privacy protections to ensure that Aadhaar and similar systems can operate securely.

⁷² Digital Personal Data Protection Act, 2023.

⁷³ Anirudh Burman 'Understanding India's New Data Protection Law' available at <https://carnegieendowment.org> accessed on 29 July 2024.

⁷⁴ Sadhya & Tanya op cit note 67.

⁷⁵ Pali et al op cit note 66.

⁷⁶ Ibid at 74.

⁷⁷ Ibid at 74.

b) The BVN security breach incident

The Bank Verification Number (BVN) breach in Nigeria serves as a significant case study highlighting the vulnerabilities of centralised biometric data systems. Managed by the Nigeria Inter-Bank Settlement System (NIBSS) under the oversight of the Central Bank of Nigeria (CBN), the BVN initiative is designed to provide a unique identifier for bank customers by linking their biometric and demographic information.⁷⁸ “It gives each bank customer a unique identity across the Nigerian Banking industry that can be used for easy identification and verification at Point of Banking operations.”⁷⁹ The project aimed to address rising cases of fraud and improve security for accessing sensitive information within the banking system. According to Esoimeme, the BVN system was introduced due to a “high demand for greater security for access to sensitive or personal information”⁸⁰ and to combat compromises on traditional security systems like passwords and PINs.

The BVN system has been lauded for its role in reducing corrupt business practices and enhancing financial security in Nigeria. A study on the impact of BVN implementation revealed its significant effect on preventing money laundering and fund diversion, particularly in monitored bank branches like those of United Bank for Africa in Abuja. The study highlights that “the implementation of BVN in 2015 helps the banking sector as well as the government of Nigeria to monitor banking transfer and transactions”.⁸¹

Despite its role in enhancing financial security, the centralisation of sensitive data introduced systemic vulnerabilities, as evidenced by the 2024 breach. Unauthorised websites, including XpressVerify.com.ng and AnyVerify.com.ng, were found offering sensitive BVN-linked information “for as little as 100 Naira.”⁸² These websites provided “access to personal and financial data, including National Identity Numbers (NINs), voter cards, and phone numbers”

⁷⁸ Central Bank of Nigeria ‘Regulatory framework for bank verification number (bvn) operations and watch-list for the nigerian banking industry’ available at <https://www.cbn.gov.ng> accessed on 30 November 2024.

⁷⁹ Olaoluwa F Onaolapo The effects of BVN on social security and credit risk (Unpublished PhD thesis, University of Lagos, 2015) 1.

⁸⁰ Ehi Esoimeme A critical analysis of the bank verification number project introduced by the central bank of Nigeria (Rudolph Kwanue University College; University of Wales System - Cardiff Law School ; James Hope University, 2015) 2.

⁸¹ M Akyuz, LW Tony & MI Opusunju ‘Impact of bank verification number (BVN) on corrupt business practices in United Bank for Africa in Abuja’ (2019) 51 *International Journal of Management Studies and Social Science Research* 39.

⁸² Ejike Kanife ‘Data breach: NIN, BVN of Nigerians sold online for just 100 naira’ available at <https://technext24.com> accessed on 29 November 2024.

.⁸³ Paradigm Initiative described this as a severe “breach of privacy rights”⁸⁴, raising concerns about identity theft, financial fraud, and national security threats.

The breach highlighted key security failures, such as insufficient encryption measures and weak oversight of third-party entities handling BVN-related data. Unauthorised access was facilitated by weak authentication mechanisms and gaps in monitoring, allowing the breach to persist undetected and exacerbating the potential damage. Investigations revealed that large-scale data leaks were possible due to systemic deficiencies in data protection and oversight frameworks.

Although “public confidence in the BVN system has been eroded”⁸⁵ due to the exposure of sensitive information, neither the CBN nor NIBSS has publicly addressed the breach or outlined any corrective measures. The incident reveals the importance of implementing the robust security protocols originally envisioned for biometric identification systems.

The BVN breach provides critical lessons for biometric data management systems like HANIS. Even systems with sophisticated biometric protections are vulnerable when encryption and data governance measures are inadequate. Nigeria’s experience demonstrates that centralised systems require continuous monitoring, strict access controls, and advanced encryption to protect sensitive information and maintain public trust. As biometric identity programs expand globally, adopting comprehensive safeguards and fostering accountability through robust legal frameworks will be essential to prevent future breaches.

8. TECHNOLOGICAL ADVANCEMENTS

Technological advancements have significantly redefined how biometric data is secured and utilised, offering scalable, efficient, and robust identity verification solutions. Biometric technologies “provide a secure method of authentication that is difficult to forge”⁸⁶, making them essential tools for verifying identities and combating crime. While these advancements present transformative opportunities, their implementation comes with challenges, including

⁸³ Paradigm Initiative ‘Major Data Breach: Sensitive Government Data of Nigerian Citizens Available Online for Just 100 Naira’ available at <https://paradigmhq.org> accessed on 29 December 2024.

⁸⁴ Paradigm op cit note 82.

⁸⁵ Ibid at 83.

⁸⁶ Marc-Julian Siewert ‘The growing role of biometrics in identity verification’ available at <https://www.biometricupdate.com> accessed on 30 November 2024.

resource constraints, ethical considerations, and the risk of algorithmic bias. For systems like HANIS, adopting these technologies must be done thoughtfully, ensuring gradual implementation, oversight, and alignment with South Africa's specific context.

a) Encryption and blockchain integration

Encryption and blockchain technologies play a critical role in protecting the integrity and confidentiality of biometric data. Encryption works by converting data into an unreadable format, accessible only to those with the correct "key."⁸⁷ The 256-bit Advanced Encryption Standard ('AES') is one such method, offering robust security for data during storage and transmission. AES encrypts data by dividing it into 128-bit chunks and transforming it into a secret format that is incomprehensible without the key. The key length can vary – 128, 192, or 256 bits – with longer keys providing higher levels of security. Widely trusted by financial and government institutions worldwide, "AES has become the standard for secret key encryption"⁸⁸ and is recognised "as secure against all known types of attacks".⁸⁹

Blockchain complements encryption by introducing a decentralised and immutable data storage structure. Unlike centralised systems, where "data is managed from a single point of control"⁹⁰, blockchain distributes data across multiple locations. This decentralised nature significantly reduces the risk of system failure or hacking, as there is no single point of vulnerability.⁹¹ Once data is added to the blockchain, it cannot be altered or manipulated, ensuring both transparency and security.

Despite these advantages, blockchain adoption for systems like HANIS must address challenges such as high energy consumption, scalability issues, and significant implementation costs. In resource-constrained settings like South Africa, adopting blockchain may require phased implementation, starting with pilot projects to evaluate feasibility and cost-effectiveness.

⁸⁷ G Popek & CS Kline 'Encryption and secure computer networks' (1979) 11 *ACM Computing Surveys* 334.

⁸⁸ D Selent 'Advanced encryption standard' (2010) 6 *Rivier Academic Journal* 1.

⁸⁹ Agne Srėbaliūtė 'AES encryption: how does it safeguard your data?' available at <https://nordlayer.com> accessed on 30 November 2024.

⁹⁰ Kenneth Proctor Decentralization, immutability, and integrity: The role of blockchain technology in enhancing cybersecurity (Thesis, Department of Cyber DevOps, University of Maryland Global Campus, 2024) 4.

⁹¹ Proctor op cit note 89.

Additionally, the integration of homomorphic encryption can further enhance privacy “by allowing computations to be performed on encrypted data without decrypting it”.⁹² This ensures that sensitive information remains confidential during data processing. While these technologies offer robust security benefits, their adoption requires substantial investment, expertise, and infrastructure upgrades – factors that must be carefully balanced against available resources.

b) Technological advancements in AI-driven biometric systems

The integration of AI into biometric systems – particularly facial recognition – has significantly enhanced security, accuracy, and efficiency. “Machine learning, a subset of AI, creates algorithms that enable systems to learn from data and make predictions without explicit programming.”⁹³ For instance, “machine learning techniques such as deep neural networks”⁹⁴ can detect subtle facial features with “high predictive accuracy, in many cases, on par with human performance”.⁹⁵

The adaptive learning capabilities of AI are especially valuable, as continuous training on diverse datasets refines a system's accuracy, allowing it to adjust to changes in facial features over time, including aging or physical alterations. To maintain optimal performance, AI systems must be continuously evaluated to ensure they deliver “outputs that align as closely as possible to the desired results”.⁹⁶ Iterative training models further improve the speed and accuracy of identification processes, making authentication nearly instantaneous and more reliable than traditional methods.

However, the deployment of AI-driven biometric systems presents several challenges that must be addressed to ensure responsible and effective implementation. One major consideration is algorithmic bias, as AI systems are only as fair as the data on which they are trained. Algorithmic bias occurs when “systematic errors in AI systems lead to unfair outcomes, such

⁹² Kurt Rohloff ‘Homomorphic Encryption – Making It Real’ available at <https://dualitytech.com> accessed on 30 December 2024.

⁹³ N Ghadge ‘Leveraging machine learning to enhance information exploration’ (2024) 11 *Machine Learning and Applications: An International Journal* 19.

⁹⁴ G Montavon, W Samek & KR Müller ‘Methods for interpreting and understanding deep neural networks’ (2018) 73 *Digital Signal Processing* 1.

⁹⁵ Montavon op cit note 93.

⁹⁶ M Rüb et al ‘A continual and incremental learning approach for tinymml on-device training using dataset distillation and model size adaption’ (2024) IEEE 7th *International Conference on Industrial Cyber-Physical Systems* 2.

as favouring or discriminating against specific demographic groups”.⁹⁷ If training datasets lack diversity or reflect systemic biases, the resulting systems may disproportionately affect certain demographic groups. For example, facial recognition algorithms have historically shown higher error rates for individuals with darker skin tones or for women compared to men. Therefore, if HANIS does fully implement facial recognition in future, it would be crucial to prioritise training its AI models on representative datasets that reflect South Africa's diverse population to ensure equity in system performance.

Ethical concerns also arise, particularly regarding privacy issues and the potential misuse of AI systems. The reliance on facial recognition for mass surveillance, for instance, could infringe on individual rights if not properly regulated. Implementing robust data governance frameworks and aligning with the POPIA are critical steps in maintaining public trust. Section 71 of POPIA highlights that “individuals should not be subject to decisions with legal consequences or significant effects based solely on automated processing, such as profiling based on location, health, or personal behaviour. Exceptions to this rule are only permissible when proper safeguards are in place, including providing individuals with opportunities to challenge automated decisions and understand the logic behind them”.⁹⁸ Therefore, any implementation of AI-driven biometric systems must ensure that these safeguards are adhered to, preventing unjust or biased outcomes.

Furthermore, implementation costs and resource constraints pose significant challenges, as AI systems require substantial investment in infrastructure, expertise, and maintenance. For a developing economy like South Africa, these costs may strain available resources, making it essential to adopt a phased and strategic approach. HANIS could start by implementing AI in high-priority areas, such as fraud prevention, before expanding to other applications.

Human oversight is another vital aspect to consider, as even the most advanced AI systems are prone to errors, particularly in edge cases or unforeseen scenarios. To mitigate this risk, HANIS must integrate mechanisms for human oversight, ensuring that users can efficiently challenge and resolve erroneous decisions. This aligns with regulatory principles outlined in section 71 of POPIA and Article 22 of the GDPR.

⁹⁷ Lubna Takruri ‘How Onfido mitigates AI bias in facial recognition’ available at <https://onfido.com> accessed on 30 July 2024.

⁹⁸ Section 71 of Protection of Personal Information Act (POPIA).

While technologies like AI and blockchain hold transformative potential, their adoption must be balanced with real-world constraints. South Africa faces unique challenges, including limited resources, legacy infrastructure, and gaps in digital literacy, particularly in rural areas.⁹⁹ To ensure that these advancements benefit all citizens, HANIS should prioritise gradual implementation through pilot projects to test feasibility and refine processes before scaling up. Capacity building is also essential, requiring investment in workforce training and partnerships with technology providers to develop the necessary expertise for successful implementation. Additionally, stakeholder collaboration is crucial; working closely with banks, regulators, and civil society organisations will ensure that technological upgrades align with user needs and legal requirements.

Modernising HANIS with AI and blockchain technologies presents an opportunity to enhance security, efficiency, and inclusivity. However, these advancements must be implemented responsibly, with careful consideration of ethical concerns, resource constraints, and the need for robust oversight. By adopting a balanced approach, South Africa can harness the benefits of technological innovation while safeguarding public trust and data security.

c) Addressing fairness and inclusivity

“The primary objective of fairness in biometrics is to identify and mitigate bias in systems that validate individual identities or characteristics such as gender.”¹⁰⁰ This is especially critical in South Africa, where systemic inequalities persist. The HANIS primarily collects biometric data from South African citizens and permanent residents, excluding undocumented residents, foreign nationals, and refugees. “This exclusion limits their access to essential financial services, such as opening bank accounts and applying for loans, which are critical for economic participation and stability.”¹⁰¹ The inability to access formal financial services perpetuates a cycle of exclusion,

⁹⁹ B Skhakhane & S Lubbe ‘Preliminaries into problems to access information - the digital divide and rural communities’ (2005) *SAJIM* 2.

¹⁰⁰ A Valdivia, JC Serrajordia & A Swianiewicz ‘There is an elephant in the room: Towards a critique on the use of fairness in biometrics’ (2023) 3 *AI and Ethics* 1409.

¹⁰¹ H Chitimira & M Ncube ‘Legislative and other selected challenges affecting financial inclusion for the poor and low-income earners in South Africa’ (2020) 64(3) *Journal of African Law* 338.

forcing these individuals to rely on informal sources that are often unregulated and costly, further entrenching economic disparities.¹⁰²

This dynamic deepens economic disparities, further marginalising vulnerable populations. While expanding HANIS to include undocumented individuals could foster financial inclusion, it also raises sensitive questions around resource allocation, policy priorities, and public trust. Policymakers must approach this issue cautiously, balancing inclusivity with the system's operational and legal constraints.

Onfido's approach to fairness and inclusivity prioritises equitable identity verification for diverse populations. "Their mission is to enable open, secure, and inclusive connections between businesses and customers worldwide."¹⁰³ Onfido addresses algorithmic bias, promotes global accessibility, and provides remote verification services to underserved communities. With mobile-first solutions¹⁰⁴, they ensure individuals can securely access services regardless of location or access to in-person verification facilities. These efforts position Onfido as an industry leader in identity verification, offering scalable and inclusive solutions for global populations.

9. CONCLUSION

The integration of biometric authentication in South Africa's banking sector marks a significant step toward enhancing security, reducing fraud, and ensuring regulatory compliance. HANIS, in collaboration with SABRIC, has improved identity verification and operational efficiency, laying a strong foundation for secure financial services.¹⁰⁵ However, its reliance on outdated infrastructure and a centralised system presents challenges that must be addressed to fully realise its potential.

A key challenge is the exclusion of marginalised citizens, such as rural residents and individuals without formal identification, from access to financial services. This exclusion perpetuates financial inequality and forces vulnerable populations to rely on informal systems. For non-citizens, financial institutions already rely on alternative verification systems to bridge

¹⁰² Chitimira & Ncube op cit note 100.

¹⁰³ Takruri op cit note 96.

¹⁰⁴ Onfido available at <https://onfido.com> accessed on 28 December 2024.

¹⁰⁵ SABRIC 'Department of Home Affairs (DHA) Online Services' available at <https://www.sabric.co.za> accessed on 25 March 2024.

the inclusion gap. Additionally, centralised data storage poses a high risk of data breaches, underscoring the need for enhanced security measures, such as advanced encryption and decentralised storage models. Lessons from the Aadhaar and BVN breaches demonstrate the dangers of centralised systems and highlight the urgent need for stronger safeguards.

South Africa's regulatory environment under POPIA presents an opportunity for modernisation through regulatory innovation and collaborative governance. Although POPIA currently "relies on command-and-control mechanisms"¹⁰⁶, its future evolution could incorporate "Data Protection Impact Assessments (DPIAs) and voluntary certification systems"¹⁰⁷, similar to those encouraged under the GDPR. The introduction of these collaborative tools, alongside regulatory sandboxes, could alleviate the burden of compliance on regulators and foster innovation within the financial sector. As "systems that require frequent prior approvals"¹⁰⁸ can create bottlenecks, collaborative models would help reduce delays and improve compliance in "resource-constrained environments"¹⁰⁹.

By modernising HANIS with decentralised models, advanced biometric authentication methods, and improved oversight mechanisms, South Africa can create a more secure and inclusive financial ecosystem for citizens and permanent residents. Complementary systems and alternative verification methods can help address the needs of non-citizens, ensuring holistic financial inclusion without conflicting with HANIS's mandate. This collaborative approach will enable banks to support diverse populations while allowing HANIS to maintain its role as a secure national identification system.

Regulatory innovation, such as the introduction of a regulatory sandbox, can further foster the development of cutting-edge biometric solutions while ensuring compliance with data protection laws. A sandbox allows financial and technology companies to test biometric solutions in real-world conditions, gathering feedback and iterating their systems without the immediate burden of full regulatory compliance.

¹⁰⁶ V Bronstein 'Prioritising command-and-control over collaborative governance: the role of the information regulator under the Protection of Personal Information Act' (2022) 25(1) *Potchefstroom Electronic Law Journal (PELJ)* 6.

¹⁰⁷ Bronstein op cit note 106.

¹⁰⁸ Ibid at 107.

¹⁰⁹ Ibid at 107.

“Testing in a live environment provides an opportunity to understand how receptive consumers are to different pricing strategies, communication channels, business models, and to the new technologies themselves. This allows firms to continually assess and iterate their business models based on the feedback they receive”.¹¹⁰

This iterative approach not only fosters innovation but also ensures real-time stakeholder engagement, including feedback from financial institutions and consumer advocacy groups. Such collaboration helps to develop biometric solutions responsibly, with user protection at their core.

Furthermore, addressing resource constraints faced by the Information Regulator is critical for effective oversight. Regulators that lack adequate capacity may struggle to enforce compliance, leading to a culture of low adherence to data protection standards. Strengthening the regulator’s capacity through increased funding, improved staffing, and capacity-building initiatives will be essential for maintaining public trust and long-term compliance.

The modernisation of HANIS is more than a technical upgrade – it represents an opportunity for South Africa to lead globally in the development of secure, inclusive, and scalable biometric systems. By addressing systemic gaps and leveraging emerging technologies within a supportive regulatory framework, South Africa can position itself as a pioneer in digital transformation, promoting financial inclusion and public trust on a national scale.

Currently, there is a lack of conclusive research in this area of law to guide practitioners in its effective application. Further legal development and research are urgently needed to advance the field and ensure that biometric innovation is matched by robust legal understanding and protections.

¹¹⁰ Financial Conduct Authority (FCA) ‘Regulatory Sandbox Lessons Learned Report’ (2017) available at <https://www.fca.org.uk> accessed on 21 November 2024.

10. BIBLIOGRAPHY

Journals

1. Adams R et al 'Drafting a Code of Conduct for research under the Protection of Personal Information Act No. 4 of 2013' (2021) 117(5-6) *South African Journal of Science* 1-3
2. Akyuz M, Tony LW & Opusunju MI 'Impact of bank verification number (BVN) on corrupt business practices in United Bank for Africa in Abuja' (2019) 51 *International Journal of Management Studies and Social Science Research* 39-52
3. Balamurugan M 'Biometric Authentication: A Double-Edged Sword for Security?' (2023) *International Journal of Science and Research* 170-173
4. Bodepudi A & Reddy M 'Cloud-based biometric authentication techniques for secure financial transactions: a review' (2020) 4(1) *International Journal of Information and Cybersecurity* 1-18
5. Bronstein V 'Prioritising command-and-control over collaborative governance: the role of the information regulator under the Protection of Personal Information Act' (2022) *Potchefstroom Electronic Law Journal (PELJ)* 1-41
6. Brown E & Piroška D 'Governing fintech and fintech as governance: The regulatory sandbox, riskwashing, and disruptive social classification' (2022) 27 *New Political Economy* 19-32
7. Chitimira H & Ncube M 'Legislative and other selected challenges affecting financial inclusion for the poor and low-income earners in South Africa' (2020) 64(3) *Journal of African Law* 337-355
8. Cornelli G et al 'Regulatory sandboxes and fintech funding: evidence from the UK' (2024) 28 *Review of Finance* 203-233
9. Dixon P 'A failure to "do no harm"--India's Aadhaar biometric ID program and its inability to protect privacy in relation to measures in Europe and the US' (2017) 7 *Health and Technology* 539-567
10. Ferrara E 'Fairness and bias in artificial intelligence: A brief survey of sources, impacts, and mitigation strategies' (2023) 6 *Sci* 1-15
11. Gautam A 'The evaluating the impact of artificial intelligence on risk management and fraud detection in the banking sector' (2023) 13 *AI, IoT and the Fourth Industrial Revolution Review* 9-18

12. Gelb A & Clark J 'Identification for development: the biometrics revolution' (2013) 315 *Center for Global Development Working Paper* 1-66
13. Ghadge N 'Leveraging machine learning to enhance information exploration' (2024) 11 *Machine Learning and Applications: An International Journal* 17-27
14. Islam S & Apu KU 'Decentralized vs. centralized database solutions in blockchain: advantages, challenges, and use cases' (2024) 3(4) *Global Mainstream Journal of Innovation* 58-68
15. Islam U et al 'Detection of distributed denial of service (ddos) attacks in IoT-based monitoring system of the banking sector using machine learning models' (2022) 14(14) *Sustainability* 8374
16. Laux D et al 'Adoption of biometric authentication systems: implications for research and practice in the deployment of end-user security systems' (2011) 21(3) *Journal of Organizational Computing and Electronic Commerce* 221-245
17. Mohammed A & Saleh BM 'Centralized database: A prerequisite for security and sustainable development in Nigeria' (2017) *International Journal of Innovative Research in Computer Science & Technology* 209-213
18. Montavon G, Samek W & Müller KR 'Methods for interpreting and understanding deep neural networks' (2018) 73 *Digital Signal Processing* 1-15
19. Morake A, Khoza L & Bokaba T 'Biometric technology in banking institutions: the customers' perspectives' (2021) 23 *South African Journal of Information Management* 1-12
20. Nnaomah UI et al 'Digital banking and financial inclusion: a review of practices in the USA and Nigeria' (2024) 6(3) *Finance & Accounting Research Journal* 463-490
21. Pali I et al 'A comprehensive survey of Aadhaar and security issues' (2020) *arXiv preprint arXiv:2007.09409* 1-12
22. Popek G & Kline CS 'Encryption and secure computer networks' (1979) 11 *ACM Computing Surveys (CSUR)* 331-356
23. Prihodova K & Hub M 'Hand-based biometric system using convolutional neural networks' (2020) 9(1) *Acta Informatica Pragensia*, 48-57
24. Rüb M et al 'A continual and incremental learning approach for tinymml on-device training using dataset distillation and model size adaption' (2024) IEEE 7th *International Conference on Industrial Cyber-Physical Systems* 1-8
25. Sadhya D & Sahu T 'A critical survey of the security and privacy aspects of the Aadhaar framework' (2024) 140 *Computers & Security* 103782

26. Selent D ‘Advanced encryption standard’ (2010) 6 *Rivier Academic Journal* 1-14
27. Shweta A et al ‘Privacy and security of Aadhaar: a computer science perspective’ (2017) *Economic and Political Weekly* 93-102
28. Skhakhane B & Lubbe S ‘Preliminaries into problems to access information—the digital divide and rural communities’ (2005) 7 *South African Journal of Information Management (SAJIM)* 1-9
29. South African Reserve Bank ‘Consultation paper on open-banking activities in the national payment system’ (2020) *National Payment System Department* 1-29
30. Tatineni S ‘Customer authentication in mobile banking—mlops practices and AI-driven biometric authentication systems’ (2022) 3.4 *Journal of Economics & Management Research* 1-5
31. Valdivia A, Serrajòrdia JC & Swianiewicz A ‘There is an elephant in the room: towards a critique on the use of fairness in biometrics’ (2023) 3 *AI and Ethics* 1407-1422

Legislation

1. Digital Personal Data Protection Act 22 of 2023
2. European Union General Data Protection Regulation (GDPR), 2016
3. Protection of Personal Information Act No 4 of 2013

Internet sources

1. Anirudh Burman ‘Understanding India’s New Data Protection Law’ available at <https://carnegieendowment.org> accessed on 29 July 2024
2. Bowyer C ‘Electronic identity verification (eIDV)—what businesses need to know’ available at <https://onfido.com> accessed on 25 August 2024
3. Central Bank of Nigeria ‘Regulatory framework for Bank Verification Number (BVN) operations and watch-list for the Nigerian banking industry’ available at <https://www.cbn.gov.ng> accessed on 30 November 2024
4. DcentAI ‘Decentralized AI for digital identity verification’ available at <https://medium.com> accessed on 29 December 2024
5. Department of Home Affairs ‘Draft Official Identity Management Policy (Public Consultation Version)’ available at <http://www.dha.gov.za> accessed on 30 July 2024

6. Department of Home Affairs ‘Strategic plan’ available at <https://www.dha.gov.za> accessed on 26 March 2024
7. Easydebit ‘Client onboarding compliance: navigating regulatory challenges with ease’ available at <https://www.easydebit.co.za> accessed on 26 March 2024
8. Fergus R ‘Facial recognition remains largely ungoverned and dangerous in Minnesota’ available at <https://www.aclu-mn.org> accessed on 25 August 2024.
9. Financial Conduct Authority (FCA) ‘Regulatory Sandbox Lessons Learned Report’ (2017) available at <https://www.fca.org.uk> accessed on 21 November 2024
10. ICO ‘Our current areas of focus for the Regulatory Sandbox’ available at <https://ico.org.uk> accessed on 30 July 2024
11. Institute for Economic Justice ‘UBIC Statement | Government needs to urgently clarify its policies on the SRD Grant, the social grant system, and Basic Income’ available at <https://iej.org.za> accessed on 28 December 2024
12. Jarratt P ‘Onfido named as a market leader in kuppingercole’s 2022 market compass: providers of verified identity’ available at <https://onfido.com> accessed on 30 July 2024
13. Kanife E ‘Data breach: NIN, BVN of Nigerians sold online for just 100 naira’ available at <https://technext24.com> accessed on 29 November 2024
14. Lawal T ‘HANIS online verification: FAQ on HANIS verification services’ available at <https://youverify.co> accessed on 24 March 2024
15. Legal Service India ‘Understanding the Aadhaar Data Breach: Causes, Consequences, and Future Safeguards’ available at <https://legalserviceindia.com> accessed on 29 August 2024
16. Nthoiwa J ‘Banks to access Home Affairs data’ available at <https://www.itweb.co.za> accessed on 20 May 2024
17. OECD ‘Regulatory sandboxes in artificial intelligence’ available at <https://www.oecd.org> accessed on 27 November 2024
18. Onfido available at <https://onfido.com> accessed on 28 December 2024
19. Onfido ‘Onfido Privacy Policy’ available at <https://onfido.com> accessed on 30 July 2024
20. Onfido ‘Regulatory Sandbox Final Report: Onfido’ available at <https://ico.org.uk> accessed on 30 July 2024
21. Panini ‘The future of biometric authentication in banking’ available at <https://www.panini.com> accessed on 29 July 2024

22. Paradigm Initiative ‘Major Data Breach: Sensitive Government Data of Nigerian Citizens Available Online for Just 100 Naira’ available at <https://paradigmhq.org> accessed on 29 December 2024
23. Rohloff K ‘Homomorphic encryption – making it real’ available at <https://dualitytech.com> accessed on 30 December 2024
24. SABRIC ‘Department of Home Affairs (DHA) Online Services’ available at <https://www.sabric.co.za> accessed on 28 March 2024
25. Siewert M ‘The growing role of biometrics in identity verification’ available at <https://www.biometricupdate.com> accessed on 30 November 2024
26. South African Government ‘Verify identity online’ available at <https://www.gov.za> accessed on 28 March 2024
27. Srèbaliūtė A ‘AES encryption: how does it safeguard your data?’ available at <https://nordlayer.com> accessed on 30 November 2024
28. Status Check ‘SASSA Implements Biometric Verification to Combat Fraud’ available at <https://statuscheck.co.za> accessed on 29 November 2024
29. Takruri L ‘How Onfido mitigates AI bias in facial recognition’ available at <https://onfido.com> accessed on 30 July 2024
30. Takruri L ‘How to verify ID easily: a comprehensive guide’ available at <https://onfido.com> accessed on 24 March 2024
31. Wiz ‘What is API security’ available at <https://www.wiz.io> accessed on 29 December 2024
32. Wolfe Systems ‘A closer look at the Aadhaar 2018 cybersecurity breach’ available at <https://wolfesystems.com.au> accessed on 19 June 2024
33. Yasar K ‘What is multifactor authentication?’ available at <https://www.techtarget.com> accessed on 29 November 2024