

A Solution to Identity Theft and Identity Fraud? PDPC Draws the Line: NRIC Numbers No Longer Acceptable for Authentication after 2026

Singapore experienced a staggering **207% surge in identity fraud in 2024**, the highest increase across the Asia-Pacific region. The rise has been largely driven by AI-powered deepfakes, account takeovers, phishing syndicates and the growing sophistication of synthetic identity fraud.

Against this backdrop, Singapore's data protection regime is entering a decisive phase. The **Personal Data Protection Commission ("PDPC")** has signalled a firm stance: **NRIC numbers can no longer be used as authentication credentials after 2026**. This move marks a significant shift in how organisations must treat national identifiers — not merely as administrative data points, but as highly sensitive personal data vulnerable to misuse.

The Rising Threat Landscape

Cybercrimes such as personal data breaches, identity theft, misuse of personal data, phishing, and scams have risen sharply in recent years.

According to Sumsu's Identity Fraud Report (November 2024), Singapore recorded a 207% increase in identity fraud cases, compared to a 121% rise across the broader Asia-Pacific region. The disproportionate spike highlights Singapore's exposure as a digital and financial hub.

High-profile breaches have further exposed systemic vulnerabilities.

In October 2025, the PDPC imposed a \$315,000 financial penalty on Marina Bay Sands Pte Ltd for breaching its Protection Obligation under the Personal Data Protection Act ("**PDPA**"). Approximately 665,495 patrons' personal data were accessed and exfiltrated by unknown threat actors. The compromised data included names and contact details and was later found offered for sale on the dark web.

Although NRIC numbers were reportedly not the primary dataset exposed in that incident, such breaches illustrate how aggregated personal data can be weaponised for phishing, impersonation, and social engineering attacks.

Earlier, in December 2024, public concern arose when users of the Accounting and Corporate Regulatory Authority's new Bizfile portal discovered that full NRIC numbers of individuals connected to Singapore-incorporated companies were searchable and viewable without login. The incident sparked widespread debate about whether NRIC numbers were being treated with sufficient sensitivity in the digital age.

Understanding the Protection Obligation under the PDPA

Section 24 of the PDPA imposes a mandatory Protection Obligation on organisations. They must make *reasonable security arrangements* to protect personal data in their possession or control against:

1. unauthorised access;
2. collection;
3. use;
4. disclosure;
5. copying;
6. modification;
7. disposal; or
8. loss of storage media.

“Reasonable” security arrangements are not static. They evolve alongside technological risks. What may have been considered adequate a decade ago — such as verifying identity using static identifiers like NRIC numbers — may no longer meet current threat standards.

The PDPC has repeatedly emphasised that national identification numbers such as NRIC, FIN and passport numbers carry heightened sensitivity because:

1. they are unique identifiers;
2. they are permanent and cannot be easily changed; and
3. they are widely used across government and private sector systems.

Once compromised, they significantly increase the risk of identity theft.

The Previous Practice: NRIC as Authentication

For years, many organisations relied on NRIC numbers (or partial NRIC numbers) as:

1. login credentials;
2. security verification questions;
3. identity confirmation during customer service calls; or
4. default usernames in online systems.

This practice was convenient but flawed.

NRIC numbers are identifiers — not secrets. They were often shared widely across institutions, printed on physical documents, and historically used in routine transactions. Treating them as authentication factors effectively turned public or semi-public identifiers into passwords.

In today’s threat environment, where data breaches are frequent and personal information circulates on underground markets, this approach is no longer defensible.

PDPC’s Authority to Tighten Regulatory Standards

Under the PDPA, the PDPC has regulatory authority to:

1. issue advisory guidelines;
2. conduct investigations;
3. impose financial penalties;
4. direct organisations to stop collecting or using personal data unlawfully; and
5. mandate remedial measures.

The PDPC’s move to disallow NRIC numbers for authentication purposes after 2026 is consistent with its mandate to strengthen organisational accountability and mitigate systemic risk.

The decision reflects three regulatory realities:

1. **Risk-based regulation** – National identifiers are inherently high-risk.
2. **Technological evolution** – Multi-factor authentication (MFA) is now the global standard.
3. **Preventive enforcement** – Regulatory intervention is necessary before identity fraud escalates further.

Financial penalties under the PDPA can reach up to 10% of an organisation's annual turnover in Singapore (subject to statutory caps), signalling that non-compliance carries serious consequences.

What Organisations Must Do Before 2026

Organisations should begin transitioning immediately. The 2026 deadline is not far away, particularly for institutions with legacy systems.

What Not to Do

- Do not use NRIC numbers as passwords or login IDs.
- Do not verify identity solely by asking for full NRIC numbers.
- Do not display full NRIC numbers in publicly accessible platforms.
- Do not collect NRIC numbers unless legally required or necessary for high-assurance verification.

What To Do

- Implement **Multi-Factor Authentication (MFA)** (e.g. OTP + device-based authentication).
- Adopt tokenisation or pseudonymisation techniques.
- Use randomly generated customer reference numbers instead of NRIC as system identifiers.
- Conduct Data Protection Impact Assessments (DPIAs).
- Update internal data governance policies and employee training.
- Review vendor contracts to ensure third-party compliance.

Potential Long-Term Solution: Moving Beyond Static Identifiers

The deeper issue is structural reliance on static identifiers.

A more sustainable solution may include:

- **passwordless authentication systems** (biometrics + device-bound cryptographic keys);
- decentralised digital identity frameworks;
- risk-based authentication models that evaluate behavioural patterns instead of static data; or
- minimisation of data collection at the outset.

Singapore has already made strides through its national digital identity ecosystem (e.g., Singpass), which relies on layered authentication rather than NRIC-based login systems. The private sector may need to follow similar architectural principles.

Conclusion

The 207% surge in identity fraud is not merely a statistic — it is a warning signal.

The PDPC's decision to prohibit the use of NRIC numbers for authentication after 2026 represents a critical recalibration of Singapore's data protection regime. It acknowledges a simple truth: **identifiers are not secrets.**

In a world of AI-driven impersonation, deepfake technology, and commoditised stolen data, relying on static national identifiers is no longer sufficient.

GATEWAY_{LAW} CORPORATION

Advocates and Solicitors | Notary Public | Commissioners for Oaths
Patent, Design and Trade Mark Agents

3 Anson Road
#24 – 02 Springleaf Tower
Singapore 079909
Telephone: (65) 62216360
Facsimile: (65) 62216375

The question is no longer whether organisations can afford to upgrade their authentication systems. The real question is whether they can afford not to.

If you are unsure of how to comply with PDPC's December 2026 deadline, we encourage you to reach out to:



Max Ng
Managing Director
Gateway Law Corporation

max.ng@gateway-law.com

Should you have any queries as to how this update may affect you or your organisation or require further information, please do not hesitate to email us.

This article is intended to highlight key legal and practical considerations regarding PDPC's new regulations concerning the protection obligations of organisations under the PDPA. It is not intended to be comprehensive, nor should it be construed as legal advice. This article is updated as of 23 February 2026.

The authors would like to express their appreciation and thanks to Lizelle Sanly Choa Dy, trainee at Gateway Law, for her assistance and contribution to this article.