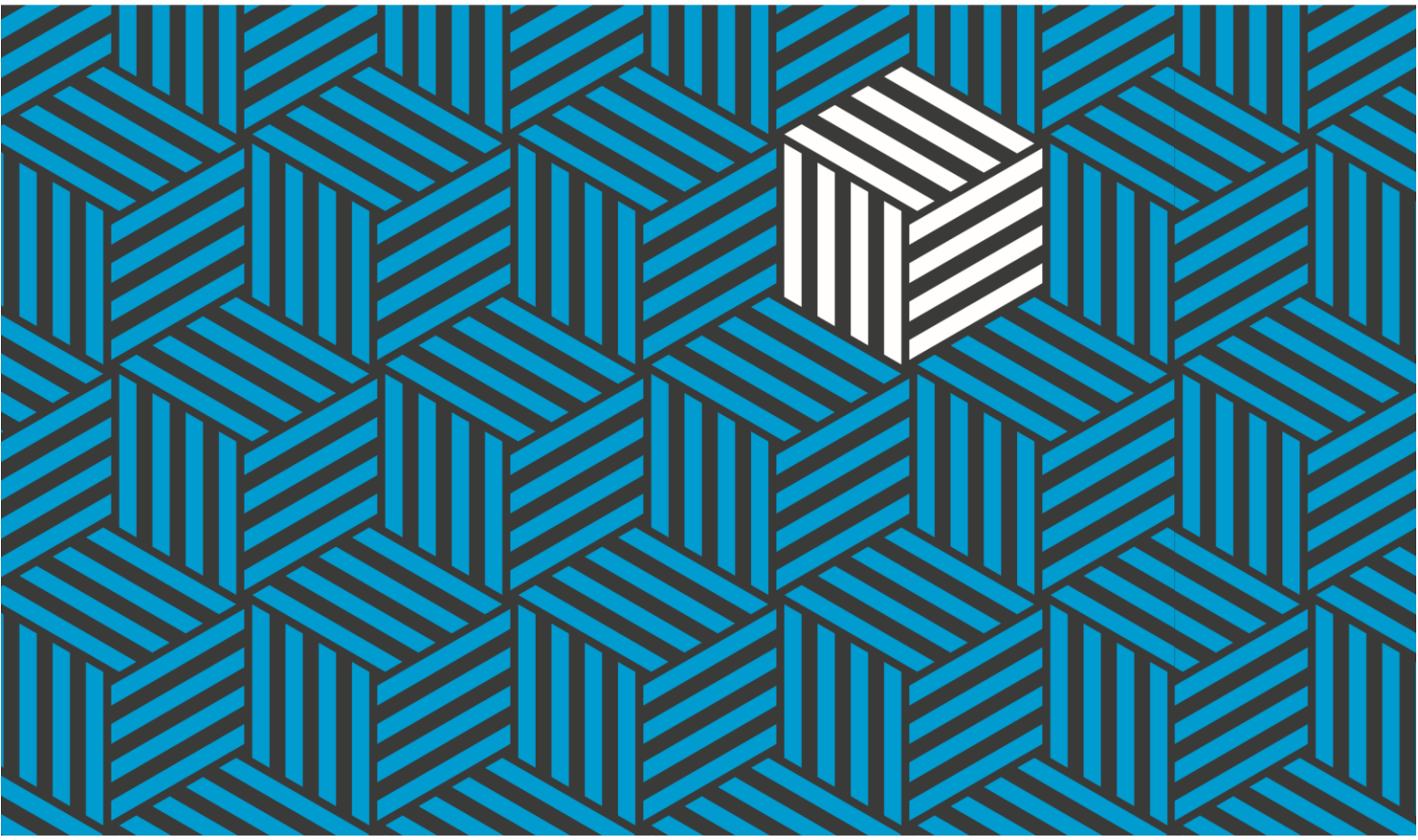
Singapore Academy of Law
Law Reform Committee

Report on Digital Identities and Legal Transactions: Part 1

March 2026



SINGAPORE ACADEMY OF LAW

Singapore Academy of Law
Law Reform Committee

Report on Digital Identities and Legal Transactions: Part I

March 2026

SINGAPORE ACADEMY OF LAW

Members of the Subcommittee

1. Allen Sng Kiat Peng
2. Violet Huang Qianwei
3. Asher Lee Jia Hern
4. Chua Kang Le

This Report was produced with the support of the Centre for Banking & Finance Law at the Faculty of Law, National University of Singapore.

Disclaimer

Whilst every effort has been made to ensure that the information contained in this report is correct, all authors, their organisations, and the Singapore Academy of Law disclaim all liability and responsibility for any error or omission in this report, and in respect of anything, or the consequences of anything, done or omitted to be done by any person in reliance, whether wholly or partially, upon the whole or any part of the contents of this report.

PREFACE

A. ABOUT THE PROJECT

1. This project is concerned with the allocation of risks and losses arising from the unauthorised use of Digital Identities. The acquisition of rights and the undertaking of liabilities are increasingly performed through digital means, and digitalisation has improved individuals' access to services and markets. Considering these benefits, governments have sought to develop the necessary digital infrastructure[1] to support users to partake in digital transactions, in particular "Digital Identities".[2]

2. As with many aspects of law and technology, while Digital Identity utilisation is developing in leaps and bounds, the laws pertaining to the use and misuse of such identities are unfortunately stuck playing "catch-up". Regulatory attention is presently focused on personal data protection[3] and little to no legislation has been made to address the transactional issues arising from the unauthorised use of Digital Identity.[4] Only in recent years have we seen more academic consideration of this area.[5]

3. The recent spates of unauthorised transactions arising from the (mis)use of Digital Identities brought to the fore difficult issues as to how such risks

---

[1] Jurisdictions such as Singapore and Estonia have a state-backed system, see Singpass website <*https://www.singpass.gov.sg/main*> (accessed 14 October 2023) and e-Estonia website <*https://e-estonia.com/solutions/e-identity/id-card/*> (accessed 14 October 2023) respectively. The UK government has recently proposed to develop a digital identities trust framework. See Government of the United Kingdom, Policy Paper on UK digital identity & attributes trust framework <*https://www.gov.uk/government/publications/uk-digital-identity-and-attributes-trust-framework-04*> (accessed 25 January 2026). There has also been a push by the UK government to adopt a state-backed system. See Kate Whannel and Henry Zeffman, "Government drops plans for mandatory digital ID to work in the UK", *British Broadcasting Corporation* (14 January 2026), <*https://www.bbc.com/news/articles/c3385zrrx73o*> (accessed 25 January 2026)

[2] See paras 32 to 36 below for a proposed concept of Digital Identities.

[3] This has, for example, led to the abolishing of the national identity register in the UK in 2010 by the Identity Documents Act 2010. See Government of the United Kingdom, Home Office, "National identity register destroyed as government consigns ID card scheme to history" (10 February 2011) <*https://www.gov.uk/government/news/national-identity-register-destroyed-as-government-consigns-id-card-scheme-to-history*> (accessed 3 February 2026). After a period of consultation, Australia has passed the Digital ID Act 2024 which, in addition to structural provisions, has a significant part dedicated at data privacy: see Digital Identity Act 2024 (AUS).

[4] In the EU, proposals to revise existing European regulation on electronic identification (Regulation (EU) No 910/2014 regarding establishing a framework for European Digital Identity [2014] OJ L 257/73, "eIDAS regulation") do not address the civil consequences of Digital Identity fraud. See Vebjørn Wold and Piia Kalamees, "Identity Theft in Consumer Finance: Consent, Contract and Liability – Analysing Rules on Loss Allocation in Norwegian, Estonian and EU Law" (2024) 11(2) Oslo Law Review 1 at 3 ("**Identity Theft in Consumer Finance**").

[5] Clare Sullivan, the foremost legal scholar in this field, has in her scholarship argued for the recognition of a right to digital identity and additional criminal law protections that may be required for the misuse of digital identity. Curiously, she does not talk about transactional liability. See Clare Sullivan, "Digital identity – From emergent legal concept to new reality" (2018) 34(4) Computer Law & Security Review 723. For more recent literature, see Identity Theft in Consumer Finance, at *supra* n 4.

and losses should be allocated to various parties in the transaction chain. In this project, the Subcommittee on Digital Identities under the Law Reform Committee of the Singapore Academy of Law (the "**Subcommittee**") seeks to provide coherent answers to two questions. Put simply:

a. Assuming that parties had done their best, as between the User and a Relying Party, who should bear the losses arising from unauthorised use of the Digital Identity;[6] and

b. What are the responsibilities of parties in the transaction chain to prevent unauthorised use and mitigate losses from such unauthorised use?[7]

B. HISTORY OF THIS PROJECT

4. On 7th November 2023, the Subcommittee published its Issues Paper on Digital Identities and Legal Transactions ("**Issues Paper"**),[8] providing an overview of this area and outlining its preliminary views regarding the issues of Primary No-Fault and Secondary Fault Liability.

5. Public consultation was conducted from 7th November 2023 to 15th April 2024, with four seminars on the Issues Paper conducted during this period. In our engagements, the main message we derived was that the current liability allocations could be improved and that reform would be much welcomed in this area. Following these engagements, the Subcommittee considered the feedback received on its Issues Paper, and issued its response to the feedback[9] on 26th August 2024.

6. While the Subcommittee was conducting its public consultation, the Monetary Authority of Singapore and the Infocomm Media Development Authority published its own consultation paper No. P016-2024 dated 25 October 2023, in respect of a proposed shared responsibility framework (the "**SRF Consultation**"). The focus of the SRF Consultation was limited to scams affecting digital payments and digital banking in Singapore. As the issues considered in the SRF Consultation are closely related to those in the Issues Paper, the Law Reform Committee provided a response to the SRF Consultation on 18 December 2023.

C. STRUCTURE OF THIS REPORT

7. The Subcommittee's review and reform recommendations will be presented as a two-part law reform report (the "**Report**"). This paper is the first part of the Report. It comprises four chapters.

---

[6] See para 42 below.
[7] See para 43 below.
[8] Law Reform Committee, Singapore Academy of Law, *Issues Paper* on Digital Identities and Legal Transactions (November 2023) ("**Issues Paper**").
[9] Law Reform Committee, Singapore Academy of Law, *Issues Paper* on Digital Identities and Legal Transactions: Response to Public Feedback (August 2024).

a. Chapter 1 develops a legal concept of Digital Identity for legal transactions, drawing on the social and legal contexts in which such Digital Identities are used.

b. Chapter 2 makes a case as to why law reform is necessary and describes the broad approach to reform which we recommend for adoption.

c. Chapter 3 deals with the allocation of Primary No-Fault Liability. Here, we make the case why this ought to be allocated to the User, provided that insurance is made available to compensate the User.

d. Chapter 4 concludes by outlining how insurance could be provided to compensate the User for unauthorised transactions entered using Digital Identities, and considers the various reform approaches to do so.

8. In the second part of the Report, we will consider the issue of Secondary Fault Liability. This will be published at a later date.

CHAPTER 1: DIGITAL IDENTITIES AND THE SOCIAL-LEGAL CONTEXT

A. DEFINING DIGITAL IDENTITY FOR LEGAL TRANSACTIONS

9. Developing a legal concept of a Digital Identity is a challenging task, given that the antecedent question of what an identity is has been the subject of much debate.[10] Even within the study of identity management, there remains disagreement about core concepts.

10. Nevertheless, it is necessary to develop such a legal concept for two reasons.

    a. First, the legal concept clarifies the scope of enquiry. The term "identity" is commonly used and carries significant importance, often causing us to overlook the challenges it presents and to fail to recognise that its various functions correspond to different meanings in diverse legal contexts.[11]

    b. Second, such a legal concept delineates what the proposed law reforms would apply to.

11. In this Chapter, we start by outlining some core concepts involved in information systems, before proposing a legal definition of Digital Identity for the purposes of this Report. We draw on two perspectives for the key features relevant to defining "Digital Identity" for the purposes of acquiring rights and undertaking obligations ("**Legal Transactions**"):

    a. First, we explain the functions of identity systems from the perspective of the state, and in particular how identity cards issued by the state facilitate commerce; and

    b. Second, we outline how technology has developed to achieve this *digitally*, in contrast to traditional identity documents. Any attempts to formulate a *legal concept* of *Digital Identity* cannot proceed in isolation, but must take into account the *legal context* in which identity documents are used, as well as the technological developments.

12. Our discussions in this Report revolve primarily on the Digital Identities of individuals. Non-natural legal persons (such as companies) act through individuals, and therefore problems ultimately regress into one involving the acts of individuals. As such, we are of the view that the insights derived from managing an individual's Digital Identity would be applicable to a non-natural legal person's Digital Identity, with appropriate modifications.

---

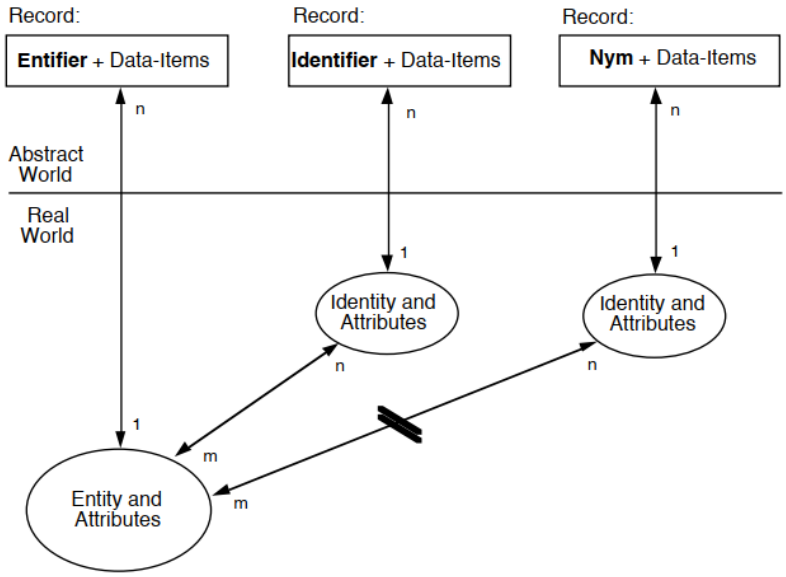
[10] See for example *Shogun Finance Ltd v Hudson* [2004] 1 AC 919, [2003] UKHL 62, where the majority of the House of Lords of the United Kingdom drew a distinction between a mistake as to "identity" and a mistake as to "attributes", with the former rendering contracts void while the latter voidable. In his dissenting judgment, Millet LJ doubted whether such a distinction can be drawn, given that a person's "identity" must "refer to a physical person, but a physical person can only be identified by describing his or her attributes", at [73].

[11] For a survey on the various contexts in which digital identity operates, the various concepts of digital identity, and the functions of digital identity, see Margarita Robles-Carrillo, "Digital identity: an approach to its nature, concept and functionalities" (2024) 32 International Journal of Law and Information Technology eaae019.

B. CORE CONCEPTS IN INFORMATION SYSTEMS

13. For the purposes of this Report, the Subcommittee has primarily adapted from works of Roger Clarke.[12] We set out a streamlined account of the salient concepts below, adapted and simplified for our present purposes.

Figure 1: Model of Human (Id)Entities and (Id)Entifiers[13]



1. Real world: Entity and Identity[14]

14. As a starting point, information systems (that is, any abstract system designed to process, store and distribute information) of all kinds recognise a

[12] In our Issues Paper, we adopted the concepts in Roger Clarke's *Identity Management: The Technologies, Their Business Value, Their Problems, Their Prospects* (Australia Capital Territory: Xamax Consultancy Pty Ltd, 2004) ("**Identity Management**"). This has been further developed over several papers. For an overview, see Roger Clarke, *A Pragmatic Model of (Id)Entity Management (IdEM)*, Series Overview (Xamax Consultancy Pte Ltd, 13 November 2023) <*https://www.rogerclarke.com/ID/IDM-O.html*> (accessed 30 January 2026). We note that Clarke's present model is much more complex than what was originally proposed in Identity Management, given his goal of providing a metatheoretic model drawing on ontology, epistemology and axiology. For our purposes, the earlier simpler model is sufficient for a working understanding of many information systems in practice. We only adapted from Clarke's more recent works where they provide important clarifications relevant to our Report.

[13] Identity Management, at p 34. We note that Clarke proposes a more complex model in his more recent work *A Reconsideration of the Foundations of Identity Management*, Bled 2022 Proceedings. Given that nothing in our analysis below turns on the additional complexity, we have retained the earlier model proposed by Clarke in Identity Management for simplicity.

[14] *Id*, at [6.2].

distinction between the real world of physical existence and the abstract world of information. In the real world, there are the following:

a. "**Entity**", which refers to a physical thing with the ability to act and be acted upon, such as cartons, animals, computers, and legal persons including individuals and companies.

b. "**Identity**", which refers to a particular presentation of an Entity, which exists as a virtual thing in the real world. An Entity may play a different role in a given context (that is, a many-to-many relationship, abbreviated as **M:N**). For example, a single individual may have an Identity of a "Customer" of a bank, but "Contractor" of a business (this is denoted by "N").[15] A given Identity may be played by many Entities, for example a "Director" of a company is a position which is occupied by different individuals over time (this is denoted by "M").

c. "**Attribute**", which refers to a characteristic of an Entity, Identity or Event. Humans will have attributes such as fingerprints, expertise, or qualifications.

d. "**Event**", which refers to an occurrence in the real world.

15. In this Report, where the term "**(Id)Entity**" is used, we refer to both Identity and Entity.

Box 1: The Entity(ies) behind Satoshi Nakamoto.

"Satoshi Nakamoto" refers to the creator of the Bitcoin System (having written the original Bitcoin code) and the author of the white paper entitled "*Bitcoin: a Peer-to-Peer Electronic Cash System*. "Satoshi Nakamoto" is estimated to hold in the region of 750,000 to 1.1 million Bitcoins.[16]

There remains considerable mystery as to who is the Entity behind "Satoshi Nakamoto".

1. Dr Craig Wright has recently laid claims that he is the sole Entity behind the Identity "Satoshi Nakamoto" although the English Courts have found that he was not the individual behind the Identity.[17]

2. It is possible that a group of individuals (rather than a single individual) are the Entities behind "Satoshi Nakamoto". In such a case, the Identity would be collectively occupied by many individuals at the same time. A loose parallel would be a joint bank account which can

[15] See para 30 and Box 5 below.
[16] See Anthony Cuthbertson, "Bitcoin creator Satoshi Nakamoto now 15th richest person in the world", *The Independent* (15 November 2021) <*https://www.independent.co.uk/tech/bitcoin-satoshi-nakamoto-wealth-net-worth-b1957878.html*> (accessed 30 January 2026).
[17] *Crypto Open Patent Alliance v Wright* [2024] EWHC 1198 (Ch) at [7].

be operated by all named account holders, and transactions from the said bank account would bind all relevant account holders.

2. Abstract world: data representing Entities and Identities[18]

16. Information systems record data (in the abstract world) about selected real-world Entities, Identities and Events, through a:

    a. "**Data-Item**", which is an element within a Record. A data-item represents a selected Attribute of an Entity, Identity or Event in the real world.

    b. "**Record**", a collection of Data-Items representing a single Entity, Identity or Event in the real world.

17. "**Entifier**" or "**Identifier**". These are each set of Data-Items that are together sufficient to distinguish a particular (Id)Entity respectively. An (Id)Entifier may enable a person to connect a Record to an (Id)Entity and distinguish one or more Records as being associated with a particular Entity or Identity (a one-to-many relationship, abbreviated as **1:N**).

18. "**Account**". An organisation manages an individual's access to data and services through an Account issued to the individual, which is a set of Data-Items that define the relationship between two parties that would include:

    a. an Identifier (such as a username or identity number);

    b. Authenticators[19] (such as a password);

    c. the permissions associated with that Identifier, which enables access to the system's resources such as data and software; and

    d. other descriptive Data-Items; and

    e. Events.

3. Nymity[20]

19. Nymity is a characteristic of an Identity that describes whether the underlying Entity may be associated with or discovered from the Identity. A transacting party with the Identity of the counterparty who wishes to know the Entity they are dealing with may encounter difficulties. That party may only have an Identifier for their counterparty and may not be able uncover the underlying Entity.

    a. Where an Identity cannot be associated with an Entity, the Identifier is categorised as an "**Anonym**" and the Identity is Anonymous.

[18] Identity Management, *supra* n 10, at [6.3].
[19] See para 22.a below.
[20] Identity Management, *supra* n 10, at [6.4].

b. Where an Identity can be associated with an Entity, but only on satisfaction of certain conditions (such as a court order to gain access to an index), the Identifier is a "**Pseudonym**" and the Identity is Pseudonymous.[21]

Box 2: Chefpierre and the Bored Ape NFT.

The facts of *Janesh s/o Rajkumar v Unknown Person* [2023] 3 SLR 1191 ("***Janesh***") illustrates some of the challenges which arise when parties are unable to go beyond an Identifier to discover the underlying Entity.

In *Janesh*, the claimant owned a non-fungible token ("**NFT**") known as the Bored Ape Yacht Club ID #2162 (the "**Bored Ape NFT**"). The claimant would enter into loan transactions with other users to borrow cryptocurrencies with NFTs as collateral, including the Bored Ape NFT. The claimant took special care when using the Bored Ape NFT as collateral, and was careful to specify terms in loan agreements that lenders whom he transacted with would not be able to take control of or claim ownership over the NFT.

The dispute in *Janesh* arose out of a loan transaction which the claimant entered into with one Chefpierre. The claimant had asked for a short extension of time to repay the loan, which Chefpierre agreed. However, Chefpierre later changed his mind and refused to enter into the refinancing loan, insisting that the current loan be repaid in full. Chefpierre transferred the Bored Ape NFT which was held in an escrow account into his cryptocurrency wallet. The Bored Ape NFT was later listed for sale on an online NFT marketplace named OpenSea.

In the case, the claimant was unable to discover the Entity behind Chefpierre – the domicile, residence and present location of the defendant were unknown.[22] Worried of possible dissipation and disposal of the Bored Ape NFT, the claimant sought a proprietary injunction against the unknown person described as: "the user behind the account "chefpierre.eth" on Twitter and Discord", and "as the person to whom the Bored Ape NFT had been transferred".[23]

Janesh provides a useful illustration of the relationship between Entities and Identities and the difficulties that arise from "Chefpierre" being an Anonym. Had the Entity behind Chefpierre been discovered (and a Pseudonym instead), the remedies available to the claimant would have been broader, such as a claim in breach of contract and damages. The practical effectiveness of

[21] See for example *CLM v CLN* [2022] 5 SLR 273 at [61] to [65], where the Entities behind certain accounts that were credited with stolen cryptocurrency assets were discovered, as a result of cryptocurrency exchanges' disclosures pursuant to disclosure orders.
[22] *Janesh s/o Rajkumar v Unknown Person* [2023] 3 SLR 1191 at [31].
[23] *Janesh s/o Rajkumar v Unknown Person* [2023] 3 SLR 1191 at [40].

the proprietary injunction obtained remains uncertain as well. While the Bored Ape NFT cannot be sold or bought on OpenSea as a result of the proprietary injunction,[24] OpenSea's help centre clarifies that OpenSea does not take custody of NFTs and despite being disabled, these NFTs may still be transferred to other wallets on the blockchain using other platforms.[25] The Bored Ape NFT is also listed on LooksRare for sale.[26]

4. (Id)Entification and (Id)Entity Authentication[27]

20. Most real-world interactions are conducted between actors with a limited amount of information about one another. In certain circumstances, there is a need by one party to know the Identity of the other. "**Identification**" refers to the process whereby data is associated with a particular Identity through the provision or acquisition of an Identifier.

21. There may be further circumstances where there is a need to strike through the Identity to reach the underlying Entity. "**Entification**" refers to the process whereby data is associated with a particular Entity through the provision or acquisition of an Entifier (such as biometrics where an Entity is an individual).

22. In an interaction where the (Id)Entity of a party matters, there is a need for the counterparty to obtain some degree of confidence in the assertion of that (Id)Entity. "**Authentication**" is carried out and refers to the process of cross-checking an assertion against one or more known evidence to establish a certain degree of confidence in an assertion.[28]

    a. An "**Authenticator**" is evidence used in the process of Authentication. An (Id)Entity Authenticator could be:

        i. **"what you know"**, such as an act demonstrating knowledge of a shared secret (a password) or ability to perform an act (a signature);

---

[24] See OpenSea website, <*https://opensea.io/assets/ethereum/0xbc4ca0eda7647a8ab7c2061c2e118a18a936f13d/2162*> (accessed 30 January 2026).

[25] OpenSea website, "Why was my NFT marked for suspicious activity?" <*https://support.opensea.io/en/articles/8867130-why-is-my-nft-marked-for-suspicious-activityy*> (accessed 25 January 2026).

[26] LooksRare website <*https://looksrare.org/collections/0xBC4CA0EdA7647A8aB7C2061c2E118A18a936f13D/2162*> (accessed 30 January 2026).

[27] Identity Management, *supra* n 10, at [6.5].

[28] Clarke opines, and we agree, that the terms "verification" or "validation" should be avoided as obtaining an absolute truth (or even a high reliability) for an (Id)Entity assertion is generally costly, intrusive, and unlikely practical in most situations. The term "Authentication", which only refers to establishing a requisite level of confidence in an assertion, is preferred. The appropriate level of confidence would vary depending on the specific transaction or circumstances. See Roger Clarke, *Extension of the Pragmatic Model of (Id)entitification to Authentication* (Xamax Consultancy Pty Ltd, 2021).

ii. "**what you have**", such as a physical or digital existence such as a Credential; or

iii. "**what you are**", such as biometrics surrendered by an individual.

b. "**Identity Authentication**" refers to the process where confidence is established in an Identity assertion, by cross-checking the assertion of Identity (that is inferred by the presentation of an Identifier) against one or more Authenticators.

c. "**Entity Authentication**", on the other hand, refers to the process whereby confidence is established in an Entity assertion. In the case of individuals, it is performed by acquiring an Entifier and cross-checking that Entifier against a pre-recorded copy of that Entifier. This is generally privacy-invasive. So an acceptable degree of confidence in an Entity assertion may not necessarily require a high level of Entity Authentication (e.g., we do not require DNA testing for the signing of contracts).

d. "**Pre-Authentication**" is the acquisition and evaluation of evidence, to establish confidence in an (Id)Entity assertion, in the registration phase, such as at Account creation.

e. "**Authorisation**" is carried out after Pre-Authentication, where an organisation determines the permissions associated with the Identity and Identifier.

f. "**Enrolment**" is carried out after Pre-Authentication, and is the recording of data into the Record of the (Id)Entity that is stored by the Account issuer.

g. "**Credential**" refers to an Authenticator issued or approved by a third-party authority recognised at law, that is trusted by the Entity, such as a registrar or notary. The authority is assumed to have undertaken some form of Authentication prior to issuing or approving the Authenticator. It may be a Document or contained in a Token.

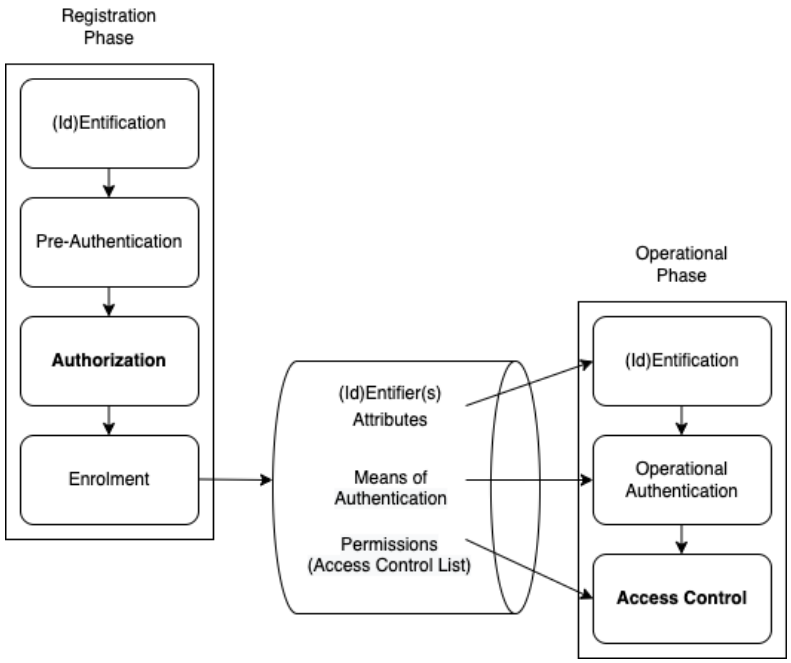
h. "**Document**" refers to an Authenticator which comprises content in any form or medium (e.g., hard-copy or soft-copy, images, video or sound). Examples include birth certificates, credit cards, statutory declarations, and letters of introduction.

i. "**Token**" refers to a recording medium on which useful data is stored, such as (Id)Entifiers, Authenticators and/or Credentials. Tokens include items storing machine-readable copies of data, and may come with built-in security features to provide confidence in its validity. Tokens are designed to provide relatively high levels of confidence in some kind of assertion, usually by including security features which prevent forgery or manipulation and are tied in some manner with a particular Entity. Examples include identity cards issued by a state which contain the biometrics of an individual, or USB hardware security keys.

23. Authentication processes may increase the degree of confidence in an assertion by using multiple Authenticators which are unrelated to one another ("**Multi-factor Authentication**"). In the context of Identity Authentication, this involves two or more different types of Identity Authenticators.

24. In totality, the process of (Id)Entity Management can be seen in Figure 2.

Figure 2: Generic Process Model of (Id)Entity Management.[29]



A. IDENTITY, THE STATE AND COMMERCE

25. The state has several policy reasons for wanting to accurately distinguish individuals from one another. In Singapore's context, the registration of individuals in Singapore and the issuing of identity cards (a Token containing a Credential) under the National Registration Act 1965 ("**NRA**") served many purposes, including as a deterrent against communist infiltration,[30] ensuring a Singapore citizen's rights to priorities in employment and social benefits,[31] tracing pawners to prevent pawning of stolen property,[32] and

[29] Roger Clarke, *A Pragmatic Model of (Id)Entity Management (IdEM) Series Overview* (Xamax Consultancy Pty Ltd) (13 November 2023) < *https://www.rogerclarke.com/ID/IDM-O.html*> (accessed 30 January 2026)
[30] Delia Teo and Clement Liew, *Guardians of our homeland: The heritage of Immigration & Checkpoints Authority* (Singapore: Immigration & Checkpoints Authority, 2004) at p 291.
[31] *Singapore Parliamentary Debates, Official Report* (30 December 1965), National Registration Act vol 24 at col 764 (Jek Yuen Thong, Minister for Labour).
[32] *Singapore Parliamentary Debates, Official Report* (14 October 1959), Registration of Persons (Amendment) Bill vol 11 at cols 705-706 (Ong Pang Boon, Minister for Home Affairs).

compiling of the electoral roll from records of existing identity documents.[33]

Box 3: Overview of the National Registration Identity Card System

What Entifiers does the state rely on to distinguish between individuals? In the registration process under the National Registration Regulations,[34] an individual applying for registration is required to provide biometric Entifiers comprising of fingerprints, photographs of face and iris scans.

Aside from biometric Entifiers, a variety of other information is also collected which may be relevant to the state for making decisions. These comprise an individual's name, place of residence, race, language/dialect, place of birth, date of birth, sex and citizenship status. Upon registration, the state will store the information collected on a national database – the register established under the NRA.[35]

The Commissioner of National Registration must then issue to the person registered under the NRA an identity card ("**NRIC**"). The NRIC contains, amongst other things, a unique state-issued Identity number (an Identifier) and the individual's photograph, fingerprint, name, race, date of birth, sex, country of birth, and address. The state-issued Identity number is an Identifier for an individual's Identity. The NRIC is a Credential as it is issued by the state.

The NRIC contains security features to safeguard against fraud (thus a Token containing a Credential). These include the use of optically variable ink, a changeable laser image of Singapore's lion head logo, and negative embossing of a lion head with microtext.[36]

26. In the context of Legal Transactions with the state where who an individual claims to be is important, the assertions by such an individual are tested through an Authentication process.

Box 4: Polling, NRICs and Authentication

Singapore citizens ordinarily resident in Singapore and are at least 21 years of age are generally entitled to vote in parliamentary and presidential

[33] *Singapore Parliamentary Debates, Official Report* (21 April 1966), Registration for the issue of new identity cards vol 25 at col 94 (Jek Yuen Thong, Minister for Labour) - "The house may be aware that the Electoral Roll has been compiled from the records of the existing identity cards."
[34] G.N. No. S226/1991, regulation 4.
[35] National Registration Act 1965, section 5.
[36] See Immigration Checkpoint Authority, "Evolution of Identity Cards" <*https://www.ica.gov.sg/about-us/our-heritage/Room/national-registration-identification*> (accessed 30 January 2026).

elections.[37] As Singapore adopts a one person, one vote system, who an individual claims to be is important in safeguarding the voting process. One such Token which may be used in the Identity and Entity Authentication process is the NRIC.

On polling day, an individual would implicitly assert that he or she is the given person entitled to ***use the Identity*** as a certain Singapore Citizen (an Identity Assertion). This is established with the individual presenting his or her NRIC as a Token during Identity Authentication. The polling officer would inspect the NRIC to ensure that the security features exist to satisfy him or herself that it is safe to rely on the Credentials contained therein (that is, the NRIC is not a forgery).

A second assertion, however, is also made by that individual – that he or she is the individual who is entitled to ***use that Credential***. This is an Entity Assertion, and is established with the individual presenting his or her biometric (in this case, the person's face). The polling officer would then check against the photograph on the NRIC to confirm that it matches the looks of the individual during the Entity Authentication process.

Only upon being so satisfied, the polling officer would provide the voter with a ballot slip for voting.

27. Given the foundational infrastructure set up by the state, businesses have found it convenient to rely on the NRIC as part of their customer onboarding process where who an individual claims to be is important. These situations include when the individual is undertaking to perform an action in the future, or the business's performance of an obligation is to a specific individual (such as transfer of assets, payment of life insurance proceeds, etc.).

28. Upon (Id)Entity Authentication, businesses would at minimum note down the individual's NRIC number in their databases. In the event of a dispute with the individual and legal proceedings must be conducted, the NRIC number becomes extremely important for two reasons:

    a. First, the NRIC number (as an Identifier) becomes an effective way to quickly describe an individual defendant whom the business is seeking to bring a claim against. This is in contrast to situations where the defendant is a "person unknown", and a claimant must resort to providing a description sufficiently certain to distinguish such a defendant.[38]

    b. Second, the NRIC number becomes an important piece of information for a judgment creditor seeking to enforce a judgment

[37] Parliamentary Elections Act 1954, section 5(1), and Presidential Elections Act 1991, section 21.
[38] See *CLM v CLN* [2022] 5 SLR 273 at [32]-[35].

obtained against an individual defendant. As institutions such as banks would similarly hold assets of a judgment debtor (such as bank deposits) against the recorded NRIC number, the NRIC number becomes integral as searches would be done against that NRIC number for the purposes of enforcement.

B. LEGAL TRANSACTIONS AND DIGITAL IDENTITY

29. As the famous adage goes, "On the internet, nobody knows you're a dog". While reliance on the NRIC issued by the state is possible for face-to-face transactions, difficulties arise when parties transact with each other remotely. The physical (Id)Entity Authentication process relies on inspecting the physical Token's security features for fraud and comparing the biometric information recorded with the person's features, both of which pose challenges when attempted to be done remotely.

30. To facilitate online transactions, businesses would issue Digital Identities to an individual for the purposes of Legal Transactions.

Box 5: Banks and Digital Identities

Traditionally, the opening of bank accounts involved a physical trip to a bank branch for onboarding. For Singapore citizens and permanent residents, this would require production of documents such as:

1. NRIC (or similar identity documents);
2. Proof of residential address (which may include the NRIC);
3. Proof of tax residency (which may include the NRIC); and
4. Proof of mobile ownership (such as a telecom bill with the customer's name and residential address).

This onboarding process associates the Identity (and Identifier) issued by the business with the individual (an Entity). Upon onboarding, the customer may seek to apply for certain Identities and corresponding Authenticators for the purposes of further remote banking transactions:

1. Automated teller machines ("**ATM**") – the customer is issued a bank /ATM/debit card, and is required to choose a password. Upon presenting the bank book/ATM/debit card and password to the ATM, the customer's Identity (as a particular customer of the business) is Authenticated and the customer is then authorised to carry out banking services (payment, cash deposits and withdrawal) through the ATM.

2. Debit/credit cards and payments – Similar to ATMs, the customer is issued a debit or credit card, and is required to choose a password and sign on the back of the debit or credit card (which are Authenticators). Payment may be made by way of such debit/credit cards upon

presentation of the card and entering a password or signing by such customer.

3. Digital banking – the customer may select a username, and is required to choose a password. Aside from the password, the customer is also required to register another Authenticator, such as a dongle producing a one-time password, or registering a phone (each of which would be a Token containing a Credential). Both the password and the Token must be presented for certain banking services to be accessible, a form of Multi-factor Authentication.

31. Traditionally, Digital Identities are only issued by organisations (such as the state or businesses) for limited purposes, typically for Legal Transactions between the organisation and its customers only. However, in recent years, Digital Identities have developed to serve much broader purposes. For example, Digital Identities have recently been issued and used to facilitate Legal Transactions between individuals and other third parties in reliance of the Digital Identities.

Box 7: Singpass and Legal Transactions

Introduction to Singpass

Singpass refers to the Digital Identity service managed by the Government Technology Agency of Singapore ("**GovTech**", a statutory board). It is linked to the state-issued Identity under the NRA. Singpass has a user base of over five million users, which is more than 97% of the Singapore Citizens and Permanent Residents aged 15 and above. Over 492 million personal and corporate transactions are facilitated via Singpass every year.[39] Singpass is used by 800 organisations offering more than 2,700 services.[40] The current suite of services includes the Singpass app, MyInfo, Verify, Identiface (a form of face verification), Login and MyInfo Business.[41]

Singpass Authentication

[39] GovTech, "Singpass: Our trusted digital identity for secure and convenient access to services" *https://www.tech.gov.sg/products-and-services/for-citizens/digital-services/singpass/* (accessed 30 January 2026).
[40] GovTech, "Singpass – Overview" <*https://www.developer.tech.gov.sg/products/categories/digital-identity/singpass/overview.html*> (accessed 25 January 2026).
[41] *Ibid*.

Singpass is based on the OpenID Connect 1.0 protocol.[42] An individual that signs up with Singpass first has their (Id)Entity Pre-Authenticated against the state database of identity as part of registration. The individual may install the Singpass app on supported smartphones, which conducts Entity Authentication using methods such as face verification. Singpass's face verification is a form of Entity Authentication, as Singpass compares the assertion to the government's records.[43] Thereafter, the smartphone will be registered as an Authenticator.

Thereafter, when an individual wishes to assert their Digital Identity to a third-party service provider (here, the Relying Party), they may be presented with Singpass Login as an Authentication method. There are two main methods to Authenticate Singpass – with a username and password, coupled with a one-time password sent to a phone number; or by scanning a displayed QR Code with a pre-registered smartphone (a Token), and presenting the correct biometrics to the same smartphone (e.g., fingerprint or facial data). Both methods use Multi-factor Authentication. Unlike Singpass's face verification, regular smartphone biometric authentication is typically **not** Entity Authentication, as it merely compares any presented biometrics to the biometrics stored locally on the device. The onus is on the device owner to ensure that no other person's biometrics are registered on the device.

Once Singpass has completed Authentication (that is, Singpass has a degree of confidence in the given Identity assertion), it communicates this degree of confidence to the Relying Party. Based on this, the Relying Party relies on the Identity Authentication conducted by Singpass and may permit the user to access an Account or resources or to conduct transactions on its platform.

<u>Government Services</u>

Singpass is used for a range of government services such as:

- the HDB portal, where users may apply for HDB flats and more.
- the CPF portal, where users may check their CPF balances, or make various applications such as for cash top-ups, CPF transfers, CPF nominations, and more.
- the HealthHub portal, where users may access their personal health records and manage appointments, payments, and medications.

[42] GovTech, "Singpass Developer Docs" <*https://docs.developer.singpass.gov.sg/docs*> (accessed 30 January 2026).
[43] Askgov, "What is Singpass Face Verification?" <*https://ask.gov.sg/singpass/questions/clul1acgh002iu36bep22rq1w?from=search*> (accessed 30 January 2026).

- the ACRA portal, where users may set up corporations or other entities, or manage existing entities under their name.
- the IRAS portal, where users view, file, and manage their taxes.

Private Sector Services

Bank accounts can be opened using the MyInfo service provided by Singpass, through which users can pre-fill Government-verified personal particulars into the necessary forms and avoid the need to submit supporting documents. This has been available since May 2017,[44] though one of the first major apps to incorporate the system was Grab, which in 2019 implemented MyInfo integration for user verification.[45]

Since July 2020, OCBC has integrated Singpass as a means for customers to access their digital banking services, the first bank to do so in Singapore.

As of today, all major banks in Singapore accept the use of Singpass to open bank accounts. One of the Subcommittee members was able to open a savings account with Standard Chartered using Singpass in less than 30 minutes, entirely online, in January 2020, though some functions were limited until the bank conducted further checks.

Singpass can also be used by businesses and customers for the digital signing of documents.[46] Businesses may register their interest by submitting a linkup request, upon which business details and compliance with technical requirements would be verified.[47] The business would then obtain a QR code, which customers may scan using Singpass to sign the document.

From 1 September 2022, an additional electronic method to effect substituted service of court documents for civil proceedings via the Singpass app inbox is made available on the eLitigation platform. Subject to obtaining permission from the Singapore Courts, subscribers of the eLitigation platform can opt for this additional method of substituted service.[48]

[44] Govtech Singapore, "Opening Bank Accounts Becomes More Seamless and Convenient for MyInfo Users" (3 May 2017) <*https://www.tech.gov.sg/media/media-releases/opening-bank-accounts-becomes-more-seamless-and-convenient-for-myinfo-users*> (accessed 30 January 2026).
[45] Grab, "Grab Creates Safer & More Secure GrabPay e-Wallet with New User Verification Feature" (7 June 2019) <*https://www.grab.com/sg/press/tech-product/grab-creates-safer-more-secure-grabpay-e-wallet-with-new-user-verification-feature/*> (accessed 30 January 2026).
[46] GovTech Singapore, "New "Sign with SingPass" service provides greater convenience in documentation signing" (4 November 2020) <*https://www.tech.gov.sg/media/media-releases/2020-11-04-sign-with-singpass*> (accessed 30 January 2026).
[47]See the Sign with Singpass webpage, "Integrate your digital services with Singpass" <https://developer.singpass.gov.sg/ (accessed 25 January 2026).
[48] Singapore Courts, "Media Release: New electronic option to effect substituted service of court documents for civil proceedings" <*https://www.judiciary.gov.sg/news-and-resources/news/news-details/media-release-new-electronic-option-to-effect-substituted-service-of-court-documents-for-civil-proceedings*> (accessed 30 January 2026).

When carrying out certain transactions, Singpass or Relying Parties may require a higher degree of confidence. As such, major retail banks in Singapore announced in September 2024 their intention for Singpass's face verification to be used in higher risk scenarios such as the setting up of digital tokens.[49] This shows a further reliance of industry on the Authentication services provided by Singpass.

C. KEY FEATURES IN THE LEGAL CONCEPT OF DIGITAL IDENTITY FOR LEGAL TRANSACTIONS

32. Having considered the core concepts in information systems, the historical context of how Identity is used by the state and the private sector for Legal Transactions, and how practices have further developed in the digital world, the Subcommittee has identified the following as key features in our legal concept of Digital Identity for Legal Transactions.

33. First, the Digital Identity must be associated with an Identifier. The Identifier would typically be a unique code or username issued by the legal person providing digital identity services (a "**Digital Identity Service Provider**"). The purpose of this is to allow Digital Identities to be distinguished from one another.

34. Second, the Digital Identity must be linked to a legal person or a group of legal persons (a "**User**"), and such linkage must be discoverable.

    a. This follows from the purpose of such Digital Identities, which is to allow parties to conduct Legal Transactions and bind such legal person(s). Without a discoverable linkage, it would be impossible for a counterparty relying on the Legal Transaction to reach the underlying legal person(s) to enforce their rights (a "**Relying Party**"). Such a linkage may be direct (the biometrics of the underlying individual is stored as part of the Digital Identity's Account), or indirect (the Identifier associated with an earlier Identity is stored as part of the Digital Identity's Account, and that earlier Identity's Account contains the biometrics of the underlying individual).

    b. We note that other legal definitions for Digital Identity (or similar concepts) have assumed that a Digital Identity is only linked to a single legal person. For example, Article 3 of the EU Regulation 910/2014 (the "eIDAS Regulation") defines "electronic identification" as meaning the process of using person identification data in electronic form ***uniquely representing either a natural or legal person, or a natural person representing a legal person***. We do not think that such a one-to-one link is necessary and have taken a

[49] "Banks to require Singpass face verification for customers setting up digital tokens" *TODAY Online* (18 September 2024) <*https://www.todayonline.com/news/banks-require-singpass-face-verification-customers-setting-digital-tokens-2481721*> (accessed 25 January 2026).

broader approach to include arrangements whereby the link is between multiple legal persons and a single Digital Identity.

35. Third, the Digital Identity, (Id)Entity Authentication and processes for entering into Legal Transactions must be recorded and carried out electronically. This is to distinguish such processes from the traditional physical processes such as (Id)Entity Authentication by way of a physical credential (for example, the physical NRIC in voting).

36. Lastly, the use of such Digital Identity must be capable of allowing Users to enter into Legal Transactions. This may either arise from that User's agreement (such as signing up for an account with a Digital Identity Service Provider and agreeing to the terms of use), or by operation of law.

CHAPTER 2: CASE FOR REFORM AND PROPOSED REFORM APPROACH

1. The case for reform

37. The use of Digital Identities for the purposes of undertaking Legal Transactions is not risk-free. With all digital technologies, there are inherent system vulnerabilities which bad actors will attempt to take advantage of. In the context of Digital Identities, actors may attempt to obtain the relevant Authenticators used to Authenticate a Digital Identity, and gain control over the Digital Identity.

Box 7: Malware, Phishing and Hacking

In Singapore, there have been several high-profile incidences involving Digital Identity and attacks on their Authenticators.

Android malware scams
Since late May 2023, victims have lost more than S$221,000 (including more than S$114,000 in CPF savings) to malware scams targeting Android mobile device users. Victims had responded to advertisements on social media platforms and were instructed to download mobile apps, resulting in malware being installed on their devices. The malware allowed bad actors to access the victims' devices remotely and obtain access to internet banking credentials, one-time passwords, and Singpass credentials. This allowed further access to the victims' bank and CPF accounts.[50]

Phishing scams
In October 2022, the Singapore Police Force warned of SMS phishing scams targeting victims for their Singpass login credentials. Unsolicited SMSes would be sent with the sender's ID containing similarities to Singpass, such as "SGSingpass". The SMSes would indicate that the recipients' Singpass accounts have been or would be deactivated, requiring the recipients to conduct facial verification. Recipients are directed to a spoofed Singpass login webpage, where they would be asked to enter their Singpass ID and password. The recipient would be led to a two-factor authenticator page asking for their Singpass one-time password, thereby granting access to bad actors. Victims have had their Singpass accounts used to sign up for bank accounts and credit cards.[51]

[50] Yasmin Begum, "Victims lose about $220,000, including CPF savings, in Android malware scams", *Channel NewsAsia* (24 June 2023) <*https://www.channelnewsasia.com/singapore/phishing-scam-malware-android-mobile-devices-cpf-savings-nine-arrested-3584666*> (accessed 2 February 2026).
[51] "Police warn of SMS phishing scams involving Singpass", *Channel NewsAsia* (2 October 2022) <*https://www.channelnewsasia.com/singapore/police-warn-sms-phishing-scams-singpass-login-details-2980726*> (accessed 2 February 2026).

Hacking

In 2021, it was reported that hackers abroad had been able to pose as 75 bank customers in Singapore to make about $500,000 in fake credit card payments. The attack involved hijacking one-time passwords sent through SMS text messages by banks. Hackers would divert such one-time passwords from banks to overseas mobile network systems, utilising them for fraudulent transactions. Bank customers did not initiate such transactions or receive the one-time passwords required to complete such transactions.[52]

38. The existence of vulnerabilities means that risks and losses must be allocated to various parties in the transaction chain, namely the User, the Digital Identity Service Provider and the Relying Party. The Subcommittee views the status quo being far from ideal and reform being warranted for two reasons.

39. First, the current state of the law reflects very divergent approaches taken on how risks and losses are allocated. There are different rules that, depending on the subject matter of the transaction, determine whether the transaction is valid and thereby allocates losses between the User and the Relying Party.[53] Losses may be shifted to other parties in the transaction chain by exceptions to these rules or other rules such as the tort of negligence (e.g., the Digital Identity Service Provider may owe a duty of care to the User/Relying party, which was breached). While the same Digital Identity may be wrongfully used to enter Legal Transactions, the outcomes may be radically different depending on what rules apply. For the uninformed member of the public, how would he or she be expected to understand the particular liability allocation under the common law, contractual agreements or statute? The liability allocation should (where possible) be one which is intuitive and simple for lay persons to understand.

40. Second, because much of the current law comprises of default rules, private orderings play an outsized role in risk and loss allocation. While private orderings could potentially reach efficient outcomes,[54] there are significant transaction costs at present which hinder such bargaining solutions. Users of Digital Identity services are unlikely to be aware of service terms and would contract with Digital Identity Service Providers on a take-it or leave-it basis. The Subcommittee notes that risks and losses are largely allocated to the Users in most of the service terms we have come across, notwithstanding that other parties in the transaction chain could take actions to reduce risk, mitigate losses, or diversify loss at a much lower cost. Clearly,

[52] Kenny Chee, "Hackers pose as bank customers by stealing OTPs, making $500k in fake credit card payments", *The Straits Times* (15 September 2021) <*https://www.straitstimes.com/tech/tech-news/hackers-pose-as-bank-customers-to-make-500k-in-fake-credit-card-payments-by-stealing*> (accessed 2 February 2026).

[53] See Chapter 3.

[54] Andrei Shleifer, "Understanding Regulation" (2005) 11(4) European Financial Management 439 at 440.

there is much merit for law reform on traditional consumer protection grounds.

Box 8: OCBC SMS Phishing Scam in 2021

In a report by Channel News Asia,[55] in December 2021, at least 469 customers of OCBC fell victim to an SMS phishing scam, losing a total of $8.5 million. These customers had received unsolicited SMSes (impersonating OCBC) which claimed that there were issues with their banking account.

The SMS would direct victims to click a link to resolve the issues, which led the victims to a fake OCBC website where victims would input their internet banking log-in details, which allowed scammers to gain control of their accounts.

OCBC subsequently made "goodwill payouts" to these victims, which covered the money they lost.

As noted by Associate Professor Hofmann in the Channel News Asia report, current bank-customer contracts often contain terms which are biased against customers, making it "practically impossible" for victims to raise defences and show that they were not liable for the losses.

This, as Associate Professor Hofmann points out, is in contrast with the approach taken under the European Union's Payments Services Directive which only allows banks to claim damages for losses incurred from fraudulent third-party transactions if it can be shown that the customer acted with gross negligence.

2. Proposed reform approach

41. The Subcommittee proposes to adopt a liability framework which draws a distinction between two different situations involving unauthorised Legal Transactions from a Digital Identity.

42. Where the situation involving unauthorised Legal Transactions from a Digital Identity does not involve any failure by any party to comply with their legal obligations, we propose that the losses (that is, the "**Primary No-Fault Liability**") should be borne by the User.

[55] Vanessa Lim & Tang See Kit, "Did OCBC set a precedent with its 'goodwill payout' for scam victims? No, lawyers say", *The Straits Times* (20 January 2022) <*https://www.channelnewsasia.com/singapore/ocbc-scam-goodwill-payout-sms-compensation-lawyers-2445061*> (accessed 2 February 2026).

43. Where fault is involved, the "**Secondary Fault Liability**" can be further classified into two categories:

    a. first, liability for failure by a transaction party to prevent such risks of unauthorised use from arising *ex ante*; and

    b. second, liability for failure by a transaction party to mitigate losses arising from such unauthorised use *ex post*.

Box 9: Primary No-Fault Liability and Secondary Fault Liability under present banking law

The distinction between Primary No-Fault Liability and Secondary Fault Liability can be illustrated with banking law.

At common law, if a bank pays out on a forged payment instrument or otherwise acts without the customer's mandate, the bank is acting outside its authority and is not entitled to debit the customer's account.[56] The Primary No-Fault Liability is allocated to the bank.

Secondary Fault Liability is allocated to the customer, when he or she fails to observe the following duties:

1. A duty to refrain from drawing a payment order or instruction in such a manner as to facilitate fraud or forgery;[57] or

2. A duty to inform the bank of any forgery or unauthorised drawing of a payment order or instruction as soon as the customer becomes aware of it.[58]

44. We note that the ***legal burden*** lies on the User to establish Secondary Fault Liability of other parties (that is, the Digital Identity Service Provider and Relying Party), in order for losses to be shifted. A party with Secondary Fault Liability may further shift losses, by establishing the Secondary Fault Liability of another party.

[56] See *Pertamina Energy Trading Limited v Credit Suisse* [2006] SGCA 26; [2006] 4 SLR(R) 273 at [51] ("***Pertamina***"), citing *Tai Hing Ltd v Liu Chong Hing Bank* [1986] 1 AC 80 at 106.
[57] *Pertamina* at [51], citing *London Joint Stock Bank, Limited v Macmillan and Arthur* [1918] AC 777.
[58] *Pertamina* at [51], citing *Greenwood (Pauper) v Martins Bank, Limited* [1933] AC 51.

CHAPTER 3: PRIMARY NO-FAULT LIABILITY

A. INTRODUCTION

45. Primary No-Fault Liability must fall on either the victim who did not authorise the transaction or the party relying on the unauthorised transaction – the classic case where one of two innocent parties must suffer for a fraud committed by someone else.

46. In this Chapter, the Subcommittee:

    a. considers a sample of rules (contract law, banking and payment law, and property law) and how they allocate Primary No-Fault Liability;

    b. distils the broad approaches taken under present law and the policy justifications for each approach; and

    c. makes a case for why the Primary No-Fault Liability for unauthorised transactions from a Digital Identity should be allocated to its User.

B. APPROACHES UNDER PRESENT LAW

47. Primary No-Fault Liability for unauthorised transactions is allocated under a variety of different rules, such as contract law, banking and payment law, and property law.[59]

1. Contract law

48. For a contract to be validly formed, there must be an act that is attributable to a party, which objectively ascertained, constituted their assent to the terms of a contract. Typically, a contracting party signifies their assent to the terms of a contract by personally affixing his or her signature. However, where a signature is forged by a fraudster, that signature would be a nullity and is incapable of binding the person whose signature is forged. *Scriptum predictum non est factum sum* – that which is claimed I wrote is not my deed.[60]

49. The act constituting assent need not be *personally performed* by a party. For example, signatures need not be personally signed, and a person may use signature machines to place signatures. Such a signature would not be a forgery, if it is applied to a document with authority of the person on whose behalf it is applied. This is best illustrated by the case of *Ramsay v Love* [2015] EWHC 65 (Ch), where the chef Gordon Ramsay was held to be bound by a personal guarantee he has not personally signed, but was signed by his

[59] For a similar survey in Estonia and Norway, see Identity Theft in Consumer Finance, *supra* n 4.
[60] *Gaillie v Lee* [1962] 2 Ch 17 per Denning MR at 30, and per Salmon LJ at 42.

father-in-law and business manager, Christopher Hutcheson, using a signature machine.

50. The rule against the imposition of liability in the absence of a voluntary act, however, is only a default rule. Parties can contract out of this default rule by expressly agreeing to alternative arrangements, subject to the limits imposed by statutes such as the Unfair Contract Terms Act 1977, Misrepresentation Act 1967, and the Consumer Protection (Fair Trading) Act 2003.[61] For instance, online platforms often include terms stating that all transactions conducted through a user's account are binding on the account holder, regardless of who actually performs the transaction. [62]

2. Banking and payments law

51. At common law, if a bank pays out on a forged payment instrument or otherwise acts without the customer's mandate, the bank is acting outside its authority and is not entitled to debit the customer's account.[63]

52. Contracting out of the above is permitted. For example, the courts have upheld banks' conclusive evidence clauses which require customers to verify bank statements and to notify the banks of any discrepancy. A customer who fails to do so within the stipulated time would be precluded from challenging the correctness of the statement.[64] Such clauses, however, are subject to controls on unfair contractual terms – the shifting of risk and liability for fraud or wilful misconduct of employees of banks by way of conclusive evidence clauses have been regarded as unreasonable under the Unfair Contract Terms Act 1977.[65]

53. Aside from the common law, there are statutes which determine the validity of certain banking transactions such as chequing.[66] A cheque is defined under the Bills of Exchange Act 1949 (2020 Rev Ed) ("**Bills of Exchange Act**") as a bill of exchange drawn on a banker payable on demand.[67] An instrument which is not signed by the person giving it is not a bill of exchange.[68] Forged or unauthorised signatures are "wholly inoperative", and banks cannot rely on them to make payment unless the customer is "precluded" from disputing his or her mandate.[69]

---

[61] For a study on how these statutes have operated in Singapore, see Sandra Booysen, "Twenty Years (and more) of Controlling Unfair Contract Terms in Singapore" [2016] SJLS 219.
[62] See for example, Singpass, "Terms of Use" *https://www.singpass.gov.sg/home/ui/terms-of-use* (accessed 31 December 2025) ("**Singpass Terms of Use**").
[63] See *Pertamina* at [52], citing *Tai Hing Ltd v Liu Chong Hing Bank* [1986] 1 AC 80 at 106.
[64] *Jiang Ou v EFG Bank AG* [2011] SGHC 149; [2011] 4 SLR 246 at [60] ("**Jiang Ou**"), citing Pertamina at [68].
[65] *Jiang Ou* at [122].
[66] See Michael Brindle and Raymond Cox, Law of Bank Payments (London: Sweet & Maxwell, 2018, 5th Ed) at [6-145] for a commentary on forged cheques and the English Bills of Exchange Act 1882.
[67] Bills of Exchange Act, section 73(1).
[68] Bills of Exchange Act, sections 3(1) and (2).
[69] Bills of Exchange Act, section 24(1).

3. Property law

54. Property law traditionally follows the maxim *nemo dat quod non habet* – a person cannot give what he or she does not have. If an asset is stolen and sold by an impostor, the original title remains unaffected and can be enforced by its owner against the subsequent purchaser. As held in *Armory v Delamirie* (1722) 1 Str 505, "the finder of a jewel, though he does not by such finding acquire an absolute property or ownership, yet he has such a property as will enable him to keep it against all but the rightful owner". Such a system protects the rights of earlier owners of property against subsequent purchasers and is termed "static security".[70] The *nemo dat* rule is also encapsulated in section 21 of the Sale of Goods Act 1979.

55. The *nemo dat* rule posed significant problems for property interests in land. A person might buy real property only to discover that the vendor was not the true owner, in which case that property could be claimed back by the true owner (such as a fraudster), and the buyer was left with an action for breach of contract against the vendor. The position for registered real property is now governed by the Land Titles Act 1993, and is based on the Torrens system which protects the rights of subsequent purchasers at the expense of prior owners of property (that is, a system of "dynamic security").[71] Subject to limited exceptions, a purchaser who acquires *registered land* for value and without fraud obtains an indefeasible title, even if the seller's title was defective,[72] effectively reversing the common law *nemo dat* approach.[73]

56. Aside from the Torrens system, the law on currency also departs from the *nemo dat* rule. At common law, while an original owner's title to notes and coins persists in the hands of a thief or anyone claiming through a thief, it is defeated by a bona fide purchaser for value. Once such notes or coins are acquired by a bona fide purchaser for value, it passes into currency and cannot be recovered.[74]

57. For completeness, we note that at common law there exists an exception to the *nemo dat* rule for sale of goods – a bona fide buyer in *market overt* obtained a new and absolute good title, regardless of the title of the seller.[75] The High Court in *Caterpillar Far East Ltd v CEL Tractors Pte Ltd* ("***Caterpillar SGHC***")[76] applied the rule by recognising the whole of Singapore as a "market overt" for some machine parts. This was overturned on appeal on

---

[70] Barry Crown, "Whither Torrens Title in Singapore?" (2010) 22 SAcLJ 9 at para 4 ("**Crown**").
[71] *Id* at para 4.
[72] Land Titles Act 1993, section 46(1).
[73] As was held in *United Overseas Bank Ltd v Bebe bte Mohammad* [2006] SGCA 30; [2006] 4 SLR(R) 884, the indefeasibility rule in the Torrens system protecting registered interests displaces the common law rule of *nemo dat*.
[74] *Miller v Race* (1758) 1 Burr. 452; *Lipkin Gorman v Karpnale Ltd* [1991] 2 A.C. 548, 572.
[75] *Caterpillar Far East Ltd v CEL Tractors Pte Ltd* [1995] SGCA 34; [1995] 1 SLR(R) 605 ("***Caterpillar SGCA***") at [12] and [21].
[76] *Caterpillar Far East Ltd v CEL Tractors Pte Ltd* [1994] SGHC 177; [1994] 2 SLR(R) 889 ("***Caterpillar SGHC***").

the basis that the rule was inapplicable in Singapore as there was neither statute or charter creating any particular market in Singapore, nor in existence any market established by prescription or custom.[77] It should also be noted that the Sale of Goods Act 1979 omits the statutory provision recognising *market overt*.[78]

4. Summary of approaches and policy considerations

58. From our survey, the approaches under present law could be mapped onto a spectrum.

Party allocated with Primary No-Fault Liability	Party relying on unauthorised transaction	Victim who did not authorise the transaction	
Areas of Law	Contract,[79] Banking,[80] and Property law[81]	Property law (real property and currency)[82] Party relying on the unauthorised transaction must have provided consideration.	Contract and banking law (private arrangements)[83]

59. In our survey, we note that there are broadly four policy considerations which inform these areas of law.

60. **A person should generally not be liable for acts not of their own**: The common law has generally preferred the protection of individual autonomy[84] and preservation of property rights.[85] As such, liability is generally

[77] Caterpillar SGCA at [22]-[23].
[78] The market overt exception in section 22 of the UK Sale of Goods Act 1979 was rendered inapplicable in Singapore by section 4(1) of the Application of English Law Act 1993. The heading of section 22 of the Singapore Sale of Goods Act 1979 has also changed over the years – "(No Operation)" in the 1994 revised edition, no heading in the 1999 revised edition and "(Repealed)" in the latest 2020 revised edition. The market overt exception was abolished in the UK by the Sale of Goods (Amendment) Act 1994.
[79] See paras 48–49 above.
[80] See paras 51 and 53 above.
[81] See para 54 above.
[82] See paras 55–56 above.
[83] See paras 50 and 52 above.
[84] See *Petelin v Cullen* [1975] 132 CLR 355 at 359, "the injustice of holding a person to a bargain to which he has not brought a consenting mind".
[85] See Ewan McKendrick, *Goode and McKendrick on Commercial Law* (London: LexisNexis, 2020, 6th Ed) at [16.05], "The common law has always strongly favoured the preservation of proprietary rights. It is an article of faith in the common law that only in exceptional cases should the owner of goods be deprived of his title to them otherwise than by his own voluntary act". See also *Bishopsgate Motor Finance Corpn Ltd v Transport Brakes Ltd* [1949] 1 KB 322, per Denning LJ at 336-337.

imposed on an individual only for their own voluntary acts. However, such protection is not absolute, as seen from the various departures.

61. **Commercial certainty:** Commerce requires that people can trust transactions once completed, especially in complex or chain transactions. If every unauthorized transaction could be easily undone, it would undermine confidence in commerce and prove disruptive to subsequent deals. Rules which allocate Primary No-Fault Liability to victims of unauthorised transactions help ensure the certainty of transactions.[86]

62. **Ability to absorb and diversify losses:** Another consideration is which party is better able to absorb losses. For example, a party relying on the unauthorised transaction might be a large institution, and is better placed to absorb losses and redistribute them amongst its other customers.[87] A victim of an unauthorised transaction may have insurance available to him or her, and could redistribute such losses amongst other insured parties.[88]

63. **Difficulties in specifying obligations, observing and establishing defaults:** Where it would be difficult to specify the obligations of a party ("**Party A**") for the purposes of Secondary Fault Liability, or where it would be difficult for another party ("**Party B**") to observe or establish defaults in court,[89] this would weigh in favour of imposing Primary No-Fault Liability on Party A. This is because doing so would mean that the prima facie losses fall on Party A, and that there is no further need to consider further whether Party A was at fault. The onus lies on Party A to show that Party B was at fault, in order to shift losses onto Party B. This would alleviate problems of incomplete specification and information asymmetry faced by one party that may arise in establishing Secondary Fault Liability of the other.

C. THE CASE FOR ALLOCATING PRIMARY NO-FAULT LIABILITY TO USERS

64. Given the above approaches, a crucial question is who should bear Primary No-fault Liability in the era of digital transacting – in particular, should the default rule favour the User or the Relying Party? We submit that on balance,

---

[86] See Crown, *supra* n 70, at para 4 in the context of real property; David Fox, "Bona Fide Purchase and the Currency of Money", The Cambridge Law Journal, Vol. 55, No. 3 (Nov. 1996), at 547–565 in the context of currency law; See also the observations of Yong CJ in *Caterpillar SGHC* in the context of the *market overt* rule, at [14] and [17].

[87] See in the context of cheque fraud *Kepitigalla Rubber Estates, Limited v National Bank of India, Limited* [1909] 2 KB 1010 at 1025, where the court observed that "the number of cases where bankers sustain losses of this kind are infinitesimal in comparison with the large business they do, and the profits of banking are sufficient to compensate them for this very small risk. To the individual customer the loss would often be very serious; to the banker it is negligible."

[88] See Crown, *supra* n 70, at paras 11-12 for the role of insurance in compensating defrauded property owners in Torrens systems. See also the observations of Yong CJ in *Caterpillar SGHC* at [17], where His Honour observed that "in the majority of cases, the original owner of the goods is covered by insurance, whereas it may be difficult for the innocent purchaser to enforce his remedy".

[89] See Hart and Moore, "Foundations of Incomplete Contracts" (1999) 66 Review of Economic Studies 115 at 118 (on observability and verifiability) and 124 (on describability).

in today's environment, the User should bear Primary No-Fault Liability in favour of commercial certainty, notwithstanding that this imposes on the Users liability for the acts of others.

65. **We note that in the era of digital contracting, unwinding transactions is highly impractical – commercial certainty is preferred.** Electronic Legal Transactions often involve rapid, back-to-back flows of funds and other Legal Transactions across multiple parties. By the time fraud is discovered, the stolen funds may have passed through several accounts or been withdrawn, especially in more complex scams where the funds would be quickly dissipated. In reliance on the unauthorised Legal Transactions, others may have entered into further Legal Transactions. If the Unauthorised Legal Transaction is unwound, this may trigger knock-on claims to set aside other Legal Transactions and engender too much uncertainty. This approach is broadly consistent with the terms of use of digital identities such as Singpass which places Primary No-Fault Liability on its users,[90] and the Monetary Authority of Singapore Shared Responsibility Framework which places Primary No-Fault Liability on account holders.[91]

66. **While we recognise that the User may not be able to absorb or diversify losses, this could be addressed through various interventions in the insurance market, which we further detail in Chapter 4**. Such an approach is not novel, and has been recommended elsewhere in the context of the real property law[92] as well as banking and payment law in Singapore.[93] While there is a risk of moral hazard arising from such insurance, we note that this is not insurmountable. Through clear specification of when Secondary Fault Liability is imposed on Users, claims could be excluded from insurance coverage if fault on the User is established by the insurer.

67. **We are of the view that there are no especial challenges in specifying the obligations, or establishing default faced by either the User or Relying Party**. The challenges in specifying the obligations appear to be broadly similar and could be overcome with various drafting techniques. On the problems of establishing default, we note that generally Users are unlikely to have necessary expertise or ability to discover whether other parties in the transaction chain are in breach of their duties. However, we are also cognisant of the fact that only a small number of Relying Parties would be sophisticated institutions (such as financial institutions), and that the vast majority would be in a similar position to Users.

---

[90] See Singpass Terms of Use, *supra* n 62, Cl 4.4 and 4.5.
[91] See Monetary Authority of Singapore, *Guidelines on Shared Responsibility Framework* (24 October 2024), and Monetary Authority of Singapore, *E-Payments User Protection Guidelines* (24 October 2024).
[92] Crown, *supra* n 70, at para 22.
[93] Sandra Booysen, "Banks and exclusion of losses for forged cheques – Is it reasonable?" (2010) 22 SAcLJ 252 at paras 24-26.

68. **The problems of establishing default are likely to be mitigated with the development of insurance coverage for Users**. The Users' claims against other parties in the transaction chain would be subrogated to the insurer after compensation, who can then investigate, pursue and even settle these claims. It would be more cost-effective for insurers to do so, given their extensive systems in-house to process claims.[94]

[94] See Richard Lewis, "*How Important are Insurers in Compensating Claims for Personal Injury in the UK?*" (2006) 31 The Geneva Papers 323, which studies the role of insurance in a system of compensation for personal injury in the UK. The same is likely to apply in Singapore.

CHAPTER 4: INSURANCE AND DIGITAL IDENTITIES

A. INTRODUCTION

69. As the Subcommittee earlier recommended the allocation of Primary No-Fault Liability to Users in the interests of commercial certainty, it is only fair that further steps be taken to ensure that Users are able to transfer (and thus diversify) some aspects of this risk.

70. In this Chapter, the Subcommittee considers:

    a. the value of insurance to Users;

    b. the market for cyber insurance;

    c. the frictions which may prevent demand for cyber insurance from being met or result in less-than-optimal demand; and

    d. the approaches which could be taken to overcome these frictions.

71. The Subcommittee notes that our analysis here is exploratory in nature. A fuller economic analysis will be necessary in order to assess whether there is indeed a missing market, the actual frictions as well as what approach is most cost-effective to address such frictions. Regulators with the support of economists would be better placed to carry out such an empirical exercise. The Subcommittee would therefore limit ourselves to outlining possible interventions that could be explored by regulators in their assessment.

B. INSURANCE AND DIGITAL IDENTITIES

1. Why insurance is valuable to Users

72. Why is the ability to transfer risks valuable? Consider the perspective of an individual User: On one end of the spectrum, Primary No-Fault Liability may result in low levels of losses, which poses only an annoyance to such individual User. More problematic, however, is the risk of significant losses, which may mean an individual User losing his or her entire life's savings.[95] In these extreme scenarios (and at the risk of oversimplification),[96] a risk adverse User would desire diversification, trading a high probability of a smaller reduction in value (that is, the insurance premium) *ex ante*, in return for avoiding a small probability of a large wipeout (that is, the coverage) *ex post*.

---

[95] See Box 7 above.

[96] For a fuller and still accessible treatment of the topic, see Sussman, *The Economics of Financial Markets & Institutions: From First Principles*, (OUP: 2023), Chapter 5.

73. In the case of company Users, their demand for insurance is more nuanced. Such demand will turn on considerations such as whether claimholders against the company's assets (such as employees, managers, suppliers, bondholders and shareholders) have a comparative advantage in obtaining diversification, the reduction of bankruptcy costs, and comparative advantages insurance firms have in processing and administering claims and loss-prevention project assessments. With these considerations in mind, while we expect some companies to have no demand for certain types of insurance, having the ability to transfer such risks will remain valuable to a great many companies.[97]

2. The market for cyber insurance

74. Presently, there does not appear to be a dedicated insurance which addresses losses arising from unauthorised Legal Transactions involving Digital Identities. Such losses are instead covered under the broader cyber insurance category.

75. Cyber insurance is a relatively novel category of insurance, covering, *inter alia,* cyber fraud and identity theft. First developed in the late 1990s in response to Y2K concerns, it seeks to address losses that ensue as a result of these cyberattacks.[98] Cyber insurance is typically offered in two forms, namely commercial and personal.

76. Commercial cyber insurance is more commonly seen as businesses are increasingly more reliant on large-scale digital infrastructure and therefore more exposed to cyber risk.[99] One survey identified five key threats that drive cyber insurance take-up—(1) ransomware; (2) business email compromise; (3) funds transfer fraud; (4) supply chain attacks and (5) effects of the COVID-19 pandemic.[100] Commercial cyber insurance may cover a large gamut of events, such as loss or damage to digital assets, business interruption, cyber extortion and forensics investigation and restoration costs.[101] In response to this burgeoning demand, the corporate cyber insurance market is projected to grow significantly worldwide in the coming years.[102] In this, it has been observed that cyber insurance has had a higher

---

[97] Mayers and Smith, "On the Corporate Demand for Insurance", (1982) 55(2) Journal of Business 190, see also Mayers and Smith, "On the Corporate Demand for Insurance: Evidence from the Reinsurance Market", (1990) 63(1) Journal of Business 19.

[98] Gilmore and Armillei, The future is now: The first wave of cyber insurance litigation commences, and the groundwork is laid for the coming storm, 2016 WL 1089828l.

[99] In a global survey by Munich Re in 2024, 51% of the respondent companies were offered commercial cyber insurance, and 41% of the respondent companies were considering taking out a cyber insurance policy and would very likely do so. In contrast, 8% of the respondent companies considered taking out a cyber insurance policy but decided against it, and 9% of the respondent companies had no plan to take out such insurance. Munich Re, *"Global Cyber Risk and Insurance Survey*", 2024 at 12.

[100] Tsohou et al, "Cyber insurance: state of the art, trends and future directions" (2023) 22 International Journal of Information Security 737 at p 739–740.

[101] *Id* at p 742.

[102] *Id* at p 743.

adoption rate in large companies as opposed to small companies, as large companies may view cyber insurance as a pre-requisite for collaboration.[103]

77. Personal cyber insurance, in contrast to its corporate counterpart, is less taken up in the market.[104] However, the increasing adoption of technology in our personal lives, driven by social media, online transactions, social networks, cloud computing and storage services, means that individuals are increasingly exposed to personal cyber risks.[105] Personal cyber insurance is a relatively recent phenomenon, driven by a realisation that individuals may actually be more vulnerable to cyber events than organisations, as organisations typically have robust cyber defence capabilities.[106] Coverage under personal cyber insurance extends to a variety of cyber-related incidents, such as fraudulent transactions made from a digital bank account or wallet, costs associated with the restoration of data, ransomware extortion and identity theft.

78. The Subcommittee briefly canvassed the state of personal cyber insurance in Singapore, and identified three personal cyber insurance offerings from eTiQa, CyberCover and FwD.

    a. eTiQa's personal cyber insurance charges a modest annual premium of $109 and covers up to $25,000 per year in losses.[107] It protects against cyber fraud, such as fraudulent transactions made from a bank account or digital wallet, as well as cyber extortion, such as ransomware attacks. It also covers costs relating to the restoration of data and in retrieving and restoring the policyholder's identity in the event of identity theft. The terms and conditions of eTiQa's cyber insurance requires a policyholder to have taken all reasonable steps to mitigate or avoid a loss under the policy. These include taking reasonable steps to safeguard computer systems, personal information, account details, and to authenticate and verify the identity of any sender of electronic communications.[108]

---

[103] *Id* at p 743.

[104] In a global survey by Munich Re in 2024, only 19% of those surveyed were offered personal cyber insurance. 36% of those surveyed were considering taking out a cyber insurance policy and would very likely do so. In contrast, 15% of those surveyed considered taking out an insurance policy but decided against it, and 42% of those surveyed had no intention of purchasing such personal cyber insurance for their private lives. Munich Re, *"Global Cyber Risk and Insurance Survey: Personal Lines*", 2024 at 21.

[105] Richard McGregor et al, "Cybersecurity and Personal Cyber Insurance: A Systematic Review" 64 Journal of Computer Information Systems 157 at 158.

[106] *Id* at 166.

[107] Personal cyber insurance, *eTiQa, <https://www.etiqa.com.sg/personal/personal-cyber-insurance/>* (accessed 25 January 2026).

[108] Personal cyber insurance, *eTiQa* at paras 4.2(b) and 4.4, <*https://www.etiqa.com.sg/wp-content/uploads/2018/08/Etiqa_Policy_Wording_TiqPersonalCyber.pdf*> (accessed 25 January 2026).

b. CyberCover, a personal cyber insurance offered by StarHub with Chubb Insurance as the underwriter, covers up to $13,000 per year for a modest monthly premium of $10.18.[109] CyberCover covers legal and other expenses relating to identity theft, cyberbullying and unauthorised transactions, and also provides buyers with protection for online transactions. Notably, its coverage for buyers protection and unauthorised transactions only goes up to $750.

c. FwD's personal cyber insurance covers up to $5,000 per incident. FwD cyber insurance comes with its home insurance schemes with no additional costs.[110] It covers online shopping fraud and fraudulent electronic transfers. FwD's policy conditions also require the policyholder to have taken reasonable measures to safeguard personal information and authenticate and verify the identity of any sender of electronic communication.[111]

79. Where the markets are able to provide for such insurance (or is likely to do so in the near future), intervention would not be necessary as parties who are risk adverse would be able to diversify their risks. To what degree is our insurance market able to provide such coverage?

80. Presently, the Subcommittee notes that the penetration rate of personal cyber insurance appears to be relatively low globally,[112] and this trend is likely to apply to Singapore as well. Similar findings were also made in the corporate cyber insurance market for small and medium-sized enterprises ("**SME**"). The 2025 QBE Singapore SME Survey shows that:[113]

a. Only 36% of the businesses have cyber insurance coverage;

b. Of the 68% of the respondents who do not have any form of insurance coverage, 51% would consider purchasing it, while 15% would categorically not consider it;

c. Only 40% of the SMEs believe that they are fully informed of cyber risks.

---

[109] Cyber cover, *Starhub,* online at: <*https://www.starhub.com/personal/mobile/mobile-phones-plans/value-added-services/cybercover.html*> (accessed 25 January 2026). See also *InsuranceBusiness,* "Chubb Singapore to provide cyber cover for StarHub customers", <*https://www.insurancebusinessmag.com/asia/news/cyber/chubb-singapore-to-provide-cyber-cover-for-starhub-customers-324600.aspx*> (accessed 25 January 2026).

[110] FwD Cyber Insurance, *FwD Insurance, <https://www.fwd.com.sg/wp-content/uploads/2023/03/FWD-Cyber-Insurance-Policy-Wording-v1.0.pdf> (accessed 25 January 2026).*

[111] *Id* at p 7.

[112] See *supra* n 103.

[113] "Singapore SMEs expect to face multiple business challenges in 2025, with over half expecting AI to significantly impact business productivity, finds QBE Singapore annual SME survey" *QBE Singapore* (17 February 2025) *<https://www.qbe.com/sg/newsroom/press-releases/qbe-singapore-sme-survey-results-business-outlook-2025>* (accessed 25 January 2026).

81. The low penetration rates suggest that there may be frictions hindering the development of such cyber insurance (that is, a missing market).

3. Frictions in the cyber insurance market

82. As a starting point, the Subcommittee notes that the insurability of a given risk is economically viable only where certain conditions are met. These include:[114]

    a. Risks being quantifiable: the probability of occurrence of a given peril, its severity and impact in terms of damages, and the requirement that losses must be assessable;

    b. A sufficiently large community with assets at risk can be established to share the risk, allowing for sufficient diversification of the risk based on differences across the community in terms of risk exposure; and

    c. The outcome of the risk must not be known to the parties (that is, unpredictable) before the provision of insurance, and is independent of the will of the insured.

83. Frictions, however, prevent these conditions from being satisfied. First, cyber risk is notoriously difficult to quantify, limiting insurers' ability to provide coverage. Attempts to provide coverage have been described as akin to "insuring aircraft in 1915 – there's a lot more that we don't know than we do know at this point".[115] Several challenges on quantifiability have been identified by the OECD[116] and the United States Government Accountability Office, including:[117]

    a. *Limited availability of historical data*: Insurance companies have faced difficulties in ascertaining historical data. Victims of cyber security incidents may be reticent to share information on such past occurrences due to reputational concerns. Furthermore, many cyber incidents tend to go unreported. This hinders the ability of insurance companies to engage in differential pricing of insurance premiums based on risk profile.

    b. *Changing nature of cyber risk*: Malicious actors continuously adapt and evolve their methods of attack to evade existing

---

[114] OECD, "Enhancing the Role of Insurance in Cyber Risk Management" (2017) <*https://www.oecd.org/en/publications/enhancing-the-role-of-insurance-in-cyber-risk-management_9789264282148-en.html*> (accessed 3 February 2026) ("**Enhancing the Role of Insurance in Cyber Risk Management**") at p 93.

[115] Matthew Sturdevant, "When Terrorists Attack Online, Is Cyber-Insurance Enough?", *GovernmentTechnology* (26 January 2015), <*https://www.govtech.com/security/when-terrorists-attack-online-is-cyber-insurance-enough.html*> (accessed 3 February 2026).

[116] Enhancing the Role of Insurance in Cyber Risk Management, *supra* n 114, at p 94 – 95.

[117] United States Government Accountability Office, "Cyber Insurance: Insurers and Policyholders Face Challenges in an Evolving Market" (May 2021) at pp 13–15, 19.

cybersecurity arrangements. This may potentially impede an accurate projection of the frequency and severity of cyberattacks. Furthermore, the application of digital technologies is also dynamic, which in turn may result in new and unpredicted areas of vulnerability and an everchanging legal framework. Therefore, insurance companies may not be able to accurately assess the vulnerability and risk profile of policyholders.

84. The problem of ***hidden type*** (or adverse selection) arising from asymmetric information between the insurer and the insured also affects the quantifiability of risk, pricing and the size of the insured persons pool.[118] Where the insurer is unable to distinguish between high-risk and low-risk applicants due to difficulties in carrying out due diligence or for applicants to credibly signal their risk type, the insurer would not be able to engage in differential pricing to cater to high-risk and low-risk individuals. Accordingly, insurers would only and would have to increase the premiums charged to the average individual. This price increase would drive low-risk individuals out of the market and leave only high-risk individuals in the market.[119]

85. Contributing to difficulties with cyber insurance is ***accumulation risk***.[120] The very concept of insurance is premised on establishing a sufficiently large pool of diversified risk to allow insurers to spread the losses. However, it is difficult to establish a diversified pool of risks for cyber insurance, given that cyber services may depend on the same infrastructure, software and services and therefore risk may be correlated. This may in turn result in a catastrophic event, when a risk manifests for many policyholders at once. For example, a vulnerability in a commonly-used software, *eg*, Singpass, may simultaneously result in losses to many policyholders. Due to the possibility of such catastrophic events, coverage for cyber risk is generally limited.

86. Further exacerbating the problem is underconsumption of insurance as a result of ***over-optimism in parties' risk assessments***, leading to a reduced insured pool. Over-optimism may lead parties to over-estimate the likelihood of positive events and underestimate the likelihood of negative events—this phenomenon is also known as optimism bias.[121] This phenomenon of optimism bias and underconsumption has also been observed in relation to cyber insurance. A study has observed that decision-makers

---

[118] See the seminal article by George Akerlof, "The Market for "Lemons": Quality uncertainty and the market mechanism" 84:3 *The Quarterly Journal of Economics* 488 at 492–494. See also Gordon et al, "A framework for using insurance for cyber-risk management", 46:3 *Communications of the ACM* 81 at 82.

[119] Enhancing the Role of Insurance in Cyber Risk Management, *supra* n 114, at p 96. See also Papatsaroucha D et al, "A survey on human and personality vulnerability assessment in cybersecurity: challenges: approaches, and open issues" 1 ACM Comput. Surv. 2021 at p 3.

[120] Enhancing the Role of Insurance in Cyber Risk Management, *supra* n 114, at pp 96–97.

[121] See Weinstein, N. D.. "Unrealistic optimism about future life events" 39(5) *Journal of Personality and Social Psychology* (1980) 806 at 806–820.

may exhibit optimism bias towards cyber risks, choosing not to adopt any additional risk management measures (such as cyber insurance) and to rely solely on self-protection.[122] This mindset often stems from a belief in the sufficiency of existing cybersecurity measures or that they are unlikely targets for cyberattacks. The study concluded that public policy interventions may thus be required to build a collaborative pool against "extreme cyber risks".[123] Optimism bias has been observed in the decision-making of both individual and corporate actors in whether to purchase cyber insurance.[124]

C. POSSIBLE INTERVENTIONS

87. In this section, the Subcommittee briefly canvasses the possible government interventions that may be appropriate to support or supplement the cyber insurance market.[125]

1. Information sharing and data collection

88. Policies may be implemented to promote, facilitate or even mandate information sharing and data collection in relation to cyber security.[126] An increased collection of flow of information would go towards resolving two issues immanent in the cyber insurance industry. First, the problem of limited availability of historical data would be ameliorated. This may assist cyber insurers to come to a more nuanced assessment of a prospective policyholder's risk profile, addressing the problem of hidden type or adverse selection arising in cyber insurance markets. Second, cyber insurers would be in a better position to analyse both macro and micro cybersecurity trends and assess its exposure, given the changing nature of cybersecurity threats.

89. There are several ways in which information flow and exchange may be facilitated, depending on its intended scope. The government may share available data held by government agencies. Data sharing between both private and public organisations may be mandated. A cyber incident data repository may even be established. An information flow and exchange scheme may be modelled after the present data protection obligations. Currently, the Personal Data Protection Act requires specified data breaches to be notified to the Personal Data Protection Commission, the failure of which may result in the imposition of financial penalties.[127] A similar notification obligation could be implemented for significant cybersecurity incidents that have occasioned actual loss, so as to facilitate data collection. The

---

[122] Martin Eling & Kwangmin Jung, "Optimism bias and its impact on cyber risk management decisions" 1 Risk Sciences (2025) at p 17.
[123] *Ibid*.
[124] *Id* at p 2, footnote 3.
[125] For a full list of the possible government interventions available to support the cyber insurance market, see Daniel Woods & Andrew Simpson, "Policy measures and cyber insurance: a framework" 2 Journal of Cyber Policy (2017) 209 ("Policy measures and cyber insurance: a framework").
[126] *Id* at p 217.
[127] See Part 6A of the Personal Data Protection Act 2012 (2020 Rev Ed).

incidents may then be compiled in a repository and made available for cyber insurance providers in assessing a prospective policyholder's risk profile and estimating prospective losses that may be occasioned by cyber security incidents. Beyond ameliorating information asymmetries, a cyber incident data repository may also provide valuable insights for cyber security agencies and organisations in the analysis of cybersecurity trends and therein enhance cybersecurity risk management.[128]

2. Catastrophic loss

90. The Government can act as an insurer of last resort.[129] This may be necessary if the private sector finds the cyber insurance industry to be inoperable or that significant government assistance is justified because it would be in the public interest. There are two possible models for the Government's intervention.

91. The Government can collect funds *ex-ante*. This can be structured by imposing a levy on general insurance policies, Digital Identity Service Providers, or even Users in general. For instance, to ensure that existing property insurance would cover terrorist acts, the UK Government set up Pool Re by imposing a levy on all household and motor policies as well as premiums to establish a fund.[130] Another example is the New Zealand Accident Compensation Corporation, which compensates citizens, residents and temporary visitors who have suffered accidental injury.[131] The accident corporation scheme is primarily funded through levies paid by workers and businesses as well as Government contributors. Modelling off these examples, a consolidated compensation fund could be established to provide compensation for Users. An obligation to contribute may be imposed on Digital Identity Service Providers, based on their risk profile as established by past cybersecurity incidents. Users may then submit claims accordingly to the consolidated compensation fund.

92. Alternatively, the Government can also recoup funds *ex-post* only after a disbursement. One example is the Terrorism Risk Insurance Act passed in the United States in 2002, in response to the 9/11 terrorist attacks.[132] Under the Act, compensation for acts of terror would be shared between the Federal Government and insurers and the US Treasury would recoup these funds by levying mandatory surcharges on specific insurance policies. In Singapore, a similar structure could be applied to cyber insurance by

---

[128] National Protection and Programs Directorate, US Department of Homeland Security, "Insurance Industry Working Session Readout Report: Insurance for Cyber-related Critical Infrastructure Loss: Key Issues" (July 2014)

[129] Policy measures and cyber insurance: a framework, *supra* n 125, at p 219.

[130] *Id*.

[131] Grant Duncan, "New Zealand's universal no-fault accident compensation scheme: Embedding community responsibility" at Jonathan Luetjens, Michael Minstrom and Paul`t Hart, eds., *Successful Public Policy*: Lessons from Australia and New Zealand (Australian National University Press, 2019) 329 at 332–334.

[132] Policy measures and cyber insurance: a framework, *supra* n 125 at p 219.

leveraging the Consolidated Fund to first compensate losses arising from the use of Digital Identities, before levying a surcharge on Digital Identity Service Providers.

3. Wider adoption

93. The Government may also implement policies to promote the wider adoption of cyber insurance. At a more surface level, the Government could consider promoting cyber insurance as a solution for the rising spate of scams.[133] This could be done through information campaigns or even offering subsidies for the purpose of purchasing cyber insurance. Beyond that, the Government can consider more interventionist policies to support the nascent cyber insurance market. For instance, the Government can exercise procurement power to support market development. This can be done by taking into consideration a company's cyber insurance or the lack thereof as a factor in deciding between tenders. This would be most appropriate for government agencies with critical security infrastructure.

94. The Government may even go so far as to mandate the purchase of cyber insurance for specific entities, *e.g.*, Digital Identity Service Providers, to cover for the losses that their Users may suffer. A comparable intervention is car insurance – in Singapore, as in many countries, car insurance is mandatory. Locally, this is operationalised by imposing an obligation on motor vehicle users to purchase insurance before a vehicle may be lawfully operated.[134] This ensures that there would be recourse to compensate for losses suffered from motor vehicle incidents. Likewise, Digital Identity Service Providers could be made to purchase cyber insurance so as to be accredited or even simply to be allowed to offer digital identity services in Singapore. This is so as to provide Users with an adequate means of recourse in the event that loss ensues.

D. ASSESSMENT OF POSSIBLE INTERVENTIONS

95. Several considerations are pertinent to which government interventions, if any, would be appropriate. These considerations would have to be canvassed in greater detail by the relevant policymaker. The Subcommittee briefly mentions two pertinent considerations.

96. The first consideration is an assessment of the economic impact that a particular intervention may have on the various actors in the market. For example, Digital Identity Service Providers have generally operated free-of-charge. The imposition of levies on Digital Identity Service Providers to create a compensation fund, for example, would inevitably result in the passing

[133] David Sun, "Scam tracker: What are the latest trends in Singapore and how much money has been lost?" *The Straits Times* (19 May 2025) <*https://www.straitstimes.com/singapore/scam-tracker-what-are-the-latest-trends-in-spore-and-how-much-money-has-been-lost*> (accessed 3 February 2026).
[134] Motor Vehicles (Third-Party Risks and Compensation) Act 1960 (2020 Rev Ed), section 3.

of costs to Users in an industry that has generally remained free. An evaluation would therefore have to be performed as to the feasibility of digital identity as a business model to ensure that the establishment of a compensation fund would not hang an albatross on the neck of Digital Identity Service Providers.

97. The second consideration is the challenges that the implementation of a particular intervention may face.

a. The creation of a compensation fund may itself result in moral hazard issues, as digital identity Users may take less precautions as a result of the compensation coverage. Therefore, the terms and conditions of the more interventionist policies would have to be carefully circumscribed to ensure that Users are incentivised to exercise due care and diligence or otherwise be disqualified from recourse to the compensation fund. Precautions that Users may be required to take may include ensuring that their passwords are sufficiently robust[135] and that their devices are secure,[136] implementing general anti-scam precautions,[137] and loss mitigation.[138]

b. Evidential difficulties in assessment would also have to be accommodated. Given that there may be significant evidential difficulties in assessing fault and causation in a cybersecurity incident, the terms and conditions of cyber insurance or a compensation fund must be tailored in a manner to reduce the evidential burden on a particular claimant. This may be done by allowing a claimant recourse to the cyber insurance or compensation fund on a no-fault basis, subject perhaps to investigations by the insurer or organisation as to any negligence on the part of the claimant. The claimant would therein have a more reasonable task of establishing its claim. One example where provisions were made to accommodate for evidential difficulties is the proposed EU AI Liability Directive (which has since been withdrawn), which suggested that a presumption of causality apply to claimants in relation to negligence claims relating to AI, to ensure that claimants would be subject to a more reasonable burden of proof and a better chance at a liability claim.[139] This presumption was premised on the difficulty in explaining and

[135] Law Reform Committee, Singapore Academy of Law, *Issues Paper* on Digital Identities and Legal Transactions (November 2023) at paras 57–59.
[136] *Ibid* at paras 63–64.
[137] *Ibid* at paras 60–62.
[138] *Ibid* at paras 63–64.
[139] Tambiama Madiega, "Artificial intelligence liability directive" *European Parliamentary Research Service* at p 6, <*https://www.europarl.europa.eu/RegData/etudes/BRIE/2023/739342/EPRS_BRI(2023)739342_EN.pdf*> (accessed 3 February 2026).

accounting for AI's autonomous behaviour, which makes proving causation difficult if not impossible for the claimant.[140]

[140] *Id* at p 3.