Singapore Academy of Law
Law Reform Committee

Issues Paper on Digital Identities and Legal Transactions

November 2023

SAL 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

An electronic copy of this report may be accessed from the Singapore Academy of Law website: *https://www.sal.org.sg/Resources-Tools/Law-Reform*.

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

About the Law Reform Committee

The Law Reform Committee of the Singapore Academy of Law makes recommendations to the authorities on the need for legislation in any particular area or subject of the law. In addition, the Subcommittee reviews any legislation before Parliament and makes recommendations for amendments to legislation (if any) and for carrying out law reform.

Comments and feedback on this report should be addressed to:

Law Reform Committee
Attn: Law Reform Co-ordinator
Singapore Academy of Law
Emails: *lawreform@sal.org.sg* and *digitalidentities@nus.edu.sg*

PREFACE

A. ABOUT THIS REVIEW

1. The acquisition of rights and 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 Digital Identity 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]

3. For example, in the UNCITRAL discussions on cross-border recognition of identity management and trust services, the working group highlighted the need to consider issues relating to transactional liability, including reliance on identity credentials, allocation of liability and broader issues of fraud and good faith.[5] However, in the latest draft instrument, provisions relating to liability only cover losses arising from Digital Identity service providers and trust service providers failing to comply with their specified

[1] Jurisdictions such as Singapore and Estonia have a state backed systems, 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, Government of the United Kingdom, Policy Paper on UK digital identity & attributes trust framework <*https://www.gov.uk/government/publications/uk-digital-identity-attributes-trust-framework-updated-version/uk-digital-identity-and-attributes-trust-framework-alpha-version-2*> (accessed 14 October 2023).

[2] See paras [31] to [35] below for a working 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 14 October 2023). Australia is now consulting on its proposed Digital Identity Legislation whereby the bulk of the discussion still focuses on privacy and personal data protection law, see Government of Australia, Australia's Digital ID System <*https://www.digitalidentity.gov.au/have-your-say*> (accessed 14 October 2023).

[4] Clara 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.

[5] See in UNCITRAL, *Report of Working Group IV (Electronic Commerce) on the work of its fifty-fifth session*, A/CN.9/902 (2017) at [75]-[80], and in UNCITRAL, *Legal Issues Related to Identity Management and Trust Services,* A/CN.9/WG.IV/WP.149 (2018) at [32(c)].

obligations.[6] This problem is also exacerbated by the recent spates of unauthorised transactions arising from the use of Digital Identities.[7]

4. The Singapore Academy of Law's Law Reform Subcommittee on Digital Identities (the "**Subcommittee**") is conducting a review into this area and the purpose of this Issues Paper is two-fold:

    a. First, we are seeking views on whether legal reform is necessary to address issues pertaining to transactions and Digital Identity, ***namely who should bear the losses from such unauthorised use, and what are the parties' responsibilities in the transaction chain to prevent unauthorised use and mitigate losses from such unauthorised use***.

    b. Second, we hope to raise public awareness on these issues identified. The research would be of interest to the general public who wish to better understand what Digital Identities are, to legal practitioners and businesses who may wish to develop their private orderings to address such issues, and to policy professionals who are advising in this area. We hope that our preliminary research in this Issues Paper will help inform any further public discussion.

5. Your feedback on this Issues Paper will be a key component of the review. This is an opportunity for stakeholders, including consumers, Digital Identity service providers, businesses, advocacy groups and legal practitioners to provide inputs on how the laws pertaining to Digital Identity and transactional liability are operating and suggestions for improvement.

B. THE REVIEW PROCESS AND MAKING A SUBMISSION

6. We are seeking the views of as many stakeholders as possible to inform our review. We have provided some questions for your consideration and discussion, and a range of issues which you may wish to consider in your submission. Neither the questions nor matters raised in this Issues Paper are intended to be exhaustive. We welcome any other suggestions or comments which you may detail in your response.

7. The closing date for submissions is 5 January 2024.

8. You may lodge your submission electronically by email at digitalidentities@nus.edu.sg. For accessibility reasons, please submit responses in a Word format. An additional PDF version may also be submitted.

9. Unless you indicate that you would like your submission to remain confidential, all information (including name and contact details) contained in

[6] See in UNCITRAL, *Draft Provisions on the Use and Cross-border Recognition of Identity Management and Trust Serviecs,* A/CN.9/WG.IV/WP.170 (2021), draft Arts. 12 and 24.
[7] See para [36] below for examples of recent incidences.

submissions may be published on the Singapore Academy of Law website. Confidential submissions must be clearly marked as confidential within the submission – automatic confidentiality statements in email are not sufficient to make your submission confidential.

CHAPTER 1: DIGITAL IDENTITIES, LEGAL TRANSACTIONS AND LIABILITY FRAMEWORK

A. DEFINING DIGITAL IDENTITY FOR LEGAL TRANSACTIONS

10. Developing a legal concept of what is a Digital Identity is a challenging task, given that the antecedent question of what is an identity has been the subject of much debate.[8] Even within the study of identity management, there remains considerable disagreement about what the core concepts are. It is necessary to develop such a legal concept for two reasons. First, the legal concept limits the scope of enquiry. The term "identity" is commonly used and carries significant importance, often causing us to overlook the challenges it presents and fail to recognise that its various functions correspond to different meanings in diverse legal contexts. Second, such a legal concept delineates what the proposed legal reforms (if any) would apply to.

11. In this Issues Paper, we start by outlining some core concepts involved in information systems. We then outline two perspectives which may inform the key features relevant to defining "Digital Identity" for the purposes of acquiring legal rights and undertaking legal obligations ("**Legal Transactions**"):

    a. First, we consider 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 consider 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. For completeness, we note that our discussions in this Issues Paper focus primarily on the Digital Identities of individuals. Non-natural legal persons (such as companies) act through individuals and therefore the 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.

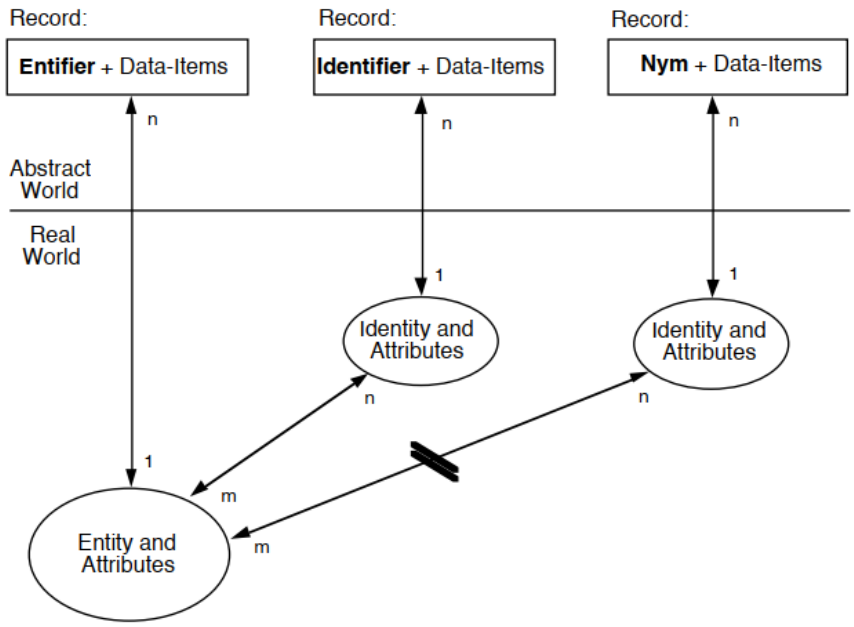
---

[8] See for example the UKHL decision of *Shogun Finance Ltd v Hudson* [2004] 1 AC 919, [2003] UKHL 62, where the majority of the UKHL 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]. For a discussion in the context of e-commerce, see Eliza Mik, "Mistaken Identity, identity theft and problems of remote authentication in e-commerce" (2012) 4 Computer Law & Security Review 28.

1. Core concepts in Information Systems

13. For the purposes of this Issues Paper, the Law Reform Subcommittee has adopted the following concepts developed by Clarke in his seminal work, *Identity Management*.[9] We reproduce a summary of the salient concepts below.

Figure 1: Model of Human (Id)Entities and (Id)Entifiers[10]



(A) Real world: Entity and Identity[11]

14. As a starting point, information systems of all kinds recognise a distinction between the real world of physical existence and the abstract world of information. In the real world, there are the following:

a. "**Attribute**", which refers to the characteristics of Entities, Identities and of Events;

b. "**Entity**", which refers to real-world things with the ability to act and be acted upon, such legal persons including individuals and companies;

c. "**Event**", which refers to an occurrence in the real world; and

[9] Roger Clarke, *Identity Management: The Technologies, Their Business Value, Their Problems, Their Prospects* (Australia Capital Territory, Xamax Consultancy Pty Ltd, 2004) ("**Identity Management**").
[10] *Id*, at p 34.
[11] *Id*, at [6.2].

d. "**Identity**", which refers to a particular presentation of an Entity. An Entity may play a different role in a given context (that is, a many-to-many relationship, abbreviated as **M:N**). For example, an individual may have an Identity of a "Customer" of a given bank.[12] 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.

15. In this Issues Paper, 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.[13]

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" and the matter has been set to be litigated in the English Courts.[14]

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

(B) Abstract world: data representing Entities and Identities[15]

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

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

[12] See para [29] and Box 5 below.
[13] 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 14 October 2023).
[14] *Crypto Open Patent Alliance v Wright* [2023] EWHC 1894 (Ch) at [2].
[15] *Identity Management*, *supra* n 9, at [6.3].

b. "**Record**", which comprises Data-Items representing an Entity or Identity in the real world; and

c. "**Transaction**", which comprises Data-Items representing an Event in the real world.

17. Among the Data-Items, some may be of particular importance, in that they may enable a person to distinguish one or more records as being associated with a particular Entity or Identity (that is, a one-to-many relationship, abbreviated as **1:N**). A set of such Data-Items is known as "**Candidate Key**". A Candidate Key for an Entity is more specifically known as an "**Entifier**", and for an Identity as an "**Identifier**". Where an Entity is an individual, the Entifier would necessarily be that individual's biometrics.

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

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

b. Authenticators[16] (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. Transactions.

(C) Nymity[17]

19. A party which wishes to know the Entity they are dealing with may encounter difficulties. That party may only have an Identifier for their counterparty, but may not be able to reach back behind it to discover the underlying Entity:

a. Where such linkage cannot be discovered at all, the Identifier is categorised as an "**Anonym**"; and

b. Where such linkage can be discovered on satisfaction of certain conditions (such as a court order to gain access to an index), the Identifier is a "**Pseudonym**".[18]

[16] See para [22.a] below.
[17] *Identity Management*, *supra* n 9, at [6.4].
[18] 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.

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 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.[19] 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 to".[20]

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 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,[21] OpenSea's help centre clarifies that OpenSea does not take custody of NFTs and despite being disabled, these NFTs may still be

[19] *Janesh s/o Rajkumar v Unknown Person* [2023] 3 SLR 1191 at [31].
[20] *Id*, at [40].
[21] See OpenSea website, <*https://opensea.io/assets/ethereum/0xbc4ca0eda7647a8ab7c2061c2e118a18a936f13d/2162*> (accessed 14 October 2023).

transferred to other wallets on the blockchain using other platforms.[22] The Bored Ape NFT is also listed on LooksRare for sale.[23]

(D) (Id)Entification and (Id)Entity Authentication[24]

20. Most interactions in the real world between actors are conducted 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 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 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 level of confidence in the assertion of that (Id)Entity, that is the process of "**Authentication**":

    a. "**Authenticator**" is evidence used in the process of Authentication. An Identity Authenticator may be:

        i. an act demonstrating knowledge (a password) or ability to perform an act (a signature);

        ii. a physical or digital existence such as a Credential, including a Token or Document; or

        iii. biometrics surrendered by an individual.

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

    c. "**Credential**" refers to an Authenticator that has physical or digital existence, such as a Document and a Token. It does not include acts such as demonstration of the possession of knowledge, or ability to perform an act.

    d. "**Document**" refers to a Credential which comprises writing or printing on paper, or its equivalent in electronic form. Examples

[22] OpenSea website, "Why was my NFT marked for suspicious activity?" <*https://support.opensea.io/hc/en-us/articles/4409456298515-Why-was-my-NFT-reported-for-suspicious-activity*> (accessed 14 October 2023).
[23] LooksRare website <*https://looksrare.org/collections/0xBC4CA0EdA7647A8aB7C2061c2E118A18a936f13D/2162*> (accessed 14 October 2023).
[24] *Identity Management*, *supra* n 9, at [6.5].

include birth certificates, credit cards, statutory declarations, and letters of introduction.

e. "**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 Entifer and cross-checking that Entifier against a pre-recorded copy of that Entifier;

f. "**Token**" refers to a Credential issued by an Entity recognised at law as having the capacity to act, to another such Entity, in which a third such Entity places some degree of trust. Tokens are designed to provide relatively high levels of confidence in some kind of assertion, usually including security features which prevent forgery 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.

23. Authentication processes may seek to increase the level of confidence in an assertion by using multiple forms of evidence ("**Multi-factor Authentication**"). In the context of Identity Authentication, this involves two or more different types of Identity Authenticators.

2. Identity, the State and Commerce

24. 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) under the National Registration Act 1965 ("**NRA**") served many purposes, including as a deterrent against communist infiltration,[25] ensuring a Singapore citizen's rights to priorities in employment and social benefits,[26] tracing pawners to prevent pawning of stolen property,[27] and compiling of the electoral roll from records of existing identity documents.[28]

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

[25] Delia Teo & Clement Liew, *Guardians of our homeland: The heritage of Immigration & Checkpoints Authority* (Singapore, Immigration & Checkpoints Authority, 2004) at p 291.
[26] *Singapore Parliamentary Debates, Official Report* (30 December 1965), National Registration Act (Jek Yuen Thong, Minister for Labour) vol 24 at col 764.
[27] *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).
[28] *Singapore Parliamentary Debates: Official Report* (21 April 1966), Registration for the issue of new identity cards (Jek Yuen Thong, Minister for Labour) vol 25 at col 94 - "The house may be aware that the Electoral Roll has been compiled from the records of the existing identity cards."

("**NRR**"),[29] an individual applying for registration is required to provide biometric Entifiers comprising of fingerprints, photograph 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.[30]

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 contains security features to safeguard against fraud (thus a Token). 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.[31]

25. 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 elections.[32] 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

[29] G.N. No. S226/1991, reg 4.
[30] National Registration Act 1965, s 5.
[31] See Immigration Checkpoint Authority, "Evolution of Identity Cards" <*https://www.ica.gov.sg/about-us/our-heritage/Room/national-registration-identification*> (accessed 14 October 2023).
[32] Parliamentary Elections Act 1954, s 5(1), and Presidential Elections Act 1991, s 21.

the NRIC to ensure that the security features exist to satisfy him or herself that it is safe to rely on the assertions 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 Token***. 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 with 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.

26. 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).

27. Upon (Id)Entity authentication, businesses would at minimum record 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.[33]

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

3. Legal Transactions and Digital Identity

28. 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

[33] See *CLM v CLN* [2022] 5 SLR 273 at [32]-[35].

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.

29. 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 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 (as a physical Token), or registering a phone (as a digital Token). Both the password and Token must be presented for certain banking services to be accessible.

30. 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 used to facilitate Legal Transactions between individuals and other parties (which are not the organisations issuing the Digital Identities).

Box 6: 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), and is linked to the state-issued Identity under the NRA. Singpass has a user base of over 4.5 million users, which is more than 97% of the Singapore Citizens and Permanent Residents aged 15 and above. Over 350 million personal and corporate transactions are facilitated via Singpass every year.[34] The current suite of services includes the Singpass app, Myinfo, Verify, Face Verification, Login and Myinfo business.[35]

Government services

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.
- 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.

A complete list of eServices can be found on the CitizenConnect website.[36]

Private Sector Services

[34] GovTech, "Factsheet – Singpass (Singapore's National Digital Identity)" (2 Mar 2022) <*https://www.smartnation.gov.sg/media-hub/press-releases/singpass-factsheet-02032022*> (accessed 14 October 2023).
[35] *Ibid*.
[36] CitizenConnect, "Find eServices" <*https://www.citizenconnectcentre.gov.sg/find-eservices/*> (accessed 14 October 2023).

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,[37] though one of the first major apps to incorporate the system was Grab, which in 2019 implemented MyInfo integration for user verification.[38]

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.[39] Businesses may register their interest by submitting a linkup request, upon which the business details and compliance with the technical requirements would be verified.[40] 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 will be 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.[41]

4. Key features relevant to developing a concept of Digital Identity for Legal Transactions

31. Taking stock of the core concepts in information systems, the historical context of how Identity is used by the state and the private sector for Legal

[37] 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 14 October 2023).
[38] 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 14 October 2023).
[39] 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 14 October 2023).
[40] See the Sign with Singpass webpage, "Introduction" <*https://api.singpass.gov.sg/library/sign/business/introduction*> (accessed 14 October 2023).
[41] 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 20 October 2023).

Transactions, and how practices have further developed in the digital world, the Subcommittee has tentatively identified the following as key features relevant in establishing a working concept of Digital Identity for Legal Transactions.

32. First, the Digital Identity must be associated with an Identifier. This would typically be a unique code or username issued by the Digital Identity provider. The purpose of this is to allow Digital Identities to be distinguished from each other.

33. 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 enter into Legal Transactions and bind such legal person(s). Without such a linkage that is discoverable, it would be impossible for a counterparty to reach to the underlying legal person(s) for the purposes of enforcing their rights. 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 Identifer associated with an Identity is stored as part of the Digital Identity's Account, and that Identity's Account contains the biometrics of the underlying individual).

    b. In addition, we note that other legal definitions for Digital Identity (or similar concepts) have assumed that a Digital Identity be 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 broader approach to include arrangements whereby the link is between multiple legal persons and a single Digital Identity.

34. Third, the Digital Identity, (Id)Entity Authentication and processes for entering into 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).

35. Last, the use of such Digital Identity must be capable of allowing legal persons to enter into Legal Transactions. This may either arise from that legal person(s) agreement (such as signing up for a bank account or SingPass and agreeing to the terms of use), or by operation of law.

Questions for Digital Identities and Legal Transactions

1. Are there perspectives, policy considerations or market practices which are not outlined above which the Subcommittee should consider in defining "Digital Identity" for Legal Transactions?

2. What are some other features which the Subcommittee should consider incorporating in the concept of Digital Identity?

3. What are some features which the Subcommittee has identified that should not be incorporated in the concept of Digital Identity?

B. PROBLEM OF UNAUTHORISED TRANSACTIONS, LIABILITY FRAMEWORK AND NEED FOR REFORM

36. 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 Andriod 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.[42]

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.[43]

Hacking

[42] 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 14 October 2023).

[43] "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 14 October 2023).

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.[44]

37. The vulnerabilities highlighted above result in difficult issues as to how such risks and losses should be allocated to various parties in the transaction chain, namely the legal persons linked to the Digital Identity, the Digital Identity service provider (who is responsible for onboarding and performing Identity Authentication), and the relying parties.

38. The Subcommittee proposes to draw a distinction between two different aspects of how such risks and losses should be allocated, turning on whether any party was at fault. Where there is no fault, the unauthorised transaction that eventuates is more akin to the occurrence of a natural disaster, and the key issue is how such losses should be fairly allocated across the parties in the transaction chain (that is, the "**Primary No-Fault Liability**").

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

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

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

    The key issue is in deciding what are the responsibilities of each party to the transaction chain, which informs when that party is at fault.

40. Whilst we have identified a few issues pertaining to Digital Identity and transactional liability, there remains a meta-issue: whether law reform is necessary in order to address these liability issues? The Subcommittee acknowledges the argument that private orderings could address these liability issues and potentially reach efficient outcomes.[45]

41. However, there may be significant transaction costs which may hinder such bargaining solutions. In particular, users of Digital Identity services are

[44] 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 14 October 2023).
[45] Andrei Shleifer, "Understanding Regulation" (2005) 11(4) European Financial Management 439 at 440.

unlikely to be aware of the service terms, and would contract with such Digital Identity service providers on a take-it or leave-it basis. Users may not have resources to enforce their rights (if any) in order to hold other parties to the transaction chain responsible, especially where the costs of enforcement are high.[46] The Subcommittee is preliminarily of the view that a case for law reform on traditional consumer protection grounds can be made out.

Questions for unauthorised transactions, liability framework and need for reform

1. Are there perspectives or policy considerations which are not outlined above which the Subcommittee should consider in developing the liability framework for unauthorised transactions?

2. Is the classification of Primary No-Fault Liability and Secondary Fault Liability appropriate?

3. Is law reform necessary to address the aforementioned issues?

[46] See para [46] below.

CHAPTER 2: PRIMARY NO-FAULT LIABILITY

42. Primary No-Fault Liability for unauthorised transactions must fall on either the User or the relying party – the classic case where one of two innocent parties must suffer for a fraud committed by someone else. What are the policy considerations which are relevant in determining which of the two parties should bear the loss?

43. First, the Subcommittee observes that the law normally only imposes liability on an individual for their own acts, but not the acts of others. As such:

    a. ***Contract law and non est factum*** – Under contract law, an individual does not become contractually bound by a document which contains his forged signature, under the doctrine of *non est factum* (that is, it is not my deed).[47]

    b. ***Banking law and customer mandates*** – Similarly, at common law, where a bank pays out upon forged cheques, that bank is acting outside of their mandate and will not be entitled to debit their customer's account.[48]

    c. ***Property law*** – Under the principle of *nemo dat quad non habet*, a person can only transfer such property interest he or she has. A fraudster impersonating another will not be able to transfer good title which he did not have. Such a system protects the rights of owners of property against subsequent purchasers and is termed static security"[49]

44. Second, the difficulty with such a position however is the countervailing need to protect innocent parties who relied upon the unauthorised transaction (that is, the need to ensure security of transactions). Given the modern-day realities where parties may enter into chains of transactions in reliance on a given transaction, it would be inimical to commerce should the law allow setting aside or reversing unauthorised transactions which may have knock-on effects on other linked transactions. As such:

    a. **Contracting out** – the law generally permits the contracting out of the earlier mentioned rules. It is common practice for banks to rely on "conclusive evidence clauses" to render a certification by a bank as to the amount owed conclusive as between the bank and the customer. As such, where a customer fails to object to the matters contained in such statement (including any unauthorised transaction), the customer is bound by such statement (subject to any challenge under the *Unfair Contract Terms Act 1977*.[50] Similarly, clause 4.3 of the Singpass Terms of Use (among other

[47] *Gallie v Lee* [1969] 2 Ch 17 per Denning MR at 30, and per Salmon LJ at 42.
[48] *Tai Hing Ltd v Liu Chong Hing Bank* [1986] 1 AC 80 at 106.
[49] Barry Crown, "Whither Torrens Title in Singapore?" (2010) 22 SAcLJ 9 at [4] ("Crown").
[50] *Jiang Ou v EFG Bank AG* [2011] 4 SLR 246 ("*Jiang Ou*").

things) deems any use or purported use of Singpass that is referrable to the associated login credentials, to be the use by the individual linked to Singpass, whether authorised or not by that individual.[51]

b. **Statutory modifications** – In the context of land law, the common law rule of *nemo dat quod non habet* is reversed under the Torrens system that was established in Singapore with the passing of the Land Titles Act 1993. Under the Torrens system, the new rule maximises security for purchasers who become proprietors of registered land (who obtains an indefeasible title, subject to limited exceptions[52]) at the expense of prior owners of interests in land.[53] Such a system is termed as dynamic security.

45. Third, the divergent approaches taken by the law highlights a further challenge: while the same Digital Identity may be wrongfully used to enter Legal Transactions, how the Primary No-Fault Liability arises from such unauthorised use of Digital Identities may well be radically different depending on the nature of the transaction. For the uninformed member of the public, how would he or she be expected to understand the particular liability allocation under common law, contractual agreements or statute? The liability allocation should (where possible) be one which is intuitive and simple for lay persons to understand.

46. Fourth, the Subcommittee considers that where it would be difficult to specify the obligations of a party ("**Party A**") for the purposes of Secondary Fault Liability, or it would be difficult for another party ("**Party B**") to observe the default or prove such breaches, this would weigh in favour of imposing the Primary No-Fault Liability on Party A. This is because doing so would mean that the prima facie losses fall on Party A and there is no further need to consider further whether Party A was at fault. The onus would lie on Party A to show that Party B was at fault, in order to shift such losses onto Party B. This would alleviate potential information asymmetry problems faced by one party that may arise in establishing Secondary Fault Liability the other party.

Box 8: OCBC SMS Phishing Scam in 2021

In a report by Channel News Asia,[54] in December 2021, at least 469 customers of OCBC fell victim to an SMS phishing scam, losing a total of $8.5 million.

[51] Singpass, "Terms of Use" <*https://www.singpass.gov.sg/home/ui/terms-of-use*> (accessed 14 October 2023) ("Singpass Terms of Use").
[52] Land Titles Act 1993, s 46(1).
[53] Crown, *supra* n 49, at [5].
[54] 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)

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 Assoc Prof 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 Assoc Prof 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.

47. Last, the Primary No-Fault Liability arising from such unauthorised use of Digital Identities should also fall on the party that is able to effectively absorb and diversify such losses. Doing so would avoid the imposition of onerous losses on any party. Relevant to such inquiry is whether there are existing insurance products available to any party in the transaction chain to diversify such losses, and whether there should be mandatory insurance as well. While there is a risk of moral hazard arising from such insurance,[55] the Subcommittee notes that this is not insurmountable, as certain claims could be excluded from insurance coverage if fault on the claimant is established.

Box 9: Cyber insurance services[56]

<*https://www.channelnewsasia.com/singapore/ocbc-scam-goodwill-payout-sms-compensation-lawyers-2445061*> (accessed 14 October 2023) ("Did OCBC set a precedent").

[55] The Central Provident Fund Board has recently stated that there is "no intent" to consider the use of insurance schemes to protect CPF members who are victims of scams involving unauthorised transactions using Singpass (presumably on the ground of moral hazard). Similarly, insurance schemes are not part of the Shared Responsibility Framework, a framework announced in February 2022 to outline an equitable way to share liabilities among parties in scam cases. See Ng Hong Siang, "'No intent' by government to consider insurance for CPF scam victims", *The Straits Times* (4 July 2023) <*https://www.channelnewsasia.com/singapore/cpf-board-insurance-scam-victims-malware-3605381*> (accessed 14 October 2023).

[56] Abigail Ng, "What is cyber insurance and can it protect scam victims", *The Straits Times* (5 September 2023) <*https://www.channelnewsasia.com/singapore/scam-insurance-phishing-online-shopping-fraud-3705286*> (accessed 14 October 2023) ("What is cyber insurance").

In Singapore, it is possible to obtain personal insurance against scams and cyber threats, although the market is still nascent. At least three companies offer cyber insurance for individuals, namely StarHub, FWD Singapore and Etiqua Insurance Singapore.

There are varying degrees of coverage under such insurances. For example, StarHub's CyberCover policy protects against fraudulent transactions made on an insured's payment card, but does not extend to unauthorised bank account transactions. The policy has a $750 limit for claims related to unauthorised transactions and online shopping, subject to the higher of a deductible of $50 or 10 per cent per claim. The policy costs $10.08 a month for individuals, or $13.11 a month for families.

FWD's insurance covers online shopping fraud and fraudulent electronic transfers, but is only available on a complimentary basis for customers who have purchased the company's home insurance product.

Etiqa's cyber insurance covers claims for stolen funds from phishing attacks, unauthorised transactions and more. The policy costs $108 annually and covers up to $25,000 per year for cyber fraud, cyber extortion, restoration costs and identity theft.

Victims who receive a refund or reimbursement from a bank will be unable to make insurance claims under these policies. For both FWD and Etiqa's coverage, confidence scams where a fraudster feigns romantic interest are also excluded.

Questions for Primary No-Fault Liability

1. Are there perspectives or policy considerations which are not outlined above which the Subcommittee should consider in recommending on whom the Primary No-Fault Liability should be allocated?

2. Given the policy considerations, as between the legal person(s) linked to the Digital Identity and the relying counterparties, who should be allocated the Primary No-Fault Liability?

3. Should there be mandatory insurance to compensate for losses that may arise from the unauthorised use of Digital Identities?

CHAPTER 3: SECONDARY FAULT LIABILITY

A. MORAL HAZARD AND POLICY CONSIDERATIONS

48. The apportionment of liability can influence the behaviour of parties, and lead to future outcomes that may be inefficient. There will be instances of loss where one party ("**Party C**") is able to take actions to reduce existing risks. In such situations, if the losses were fully apportioned to another party in the transaction chain ("**Party D**"), a rational Party C would have no incentive to reduce risks, even if the cost of taking care was lower than the expected loss prevented.

49. This is a classic case of moral hazard, whereby the costs associated with the actions of a risk-taking party (such as Party C) are not fully internalised, but are instead borne by another party (such as Party D). As such, Party C may be incentivised to take excessive risks, given that the costs are borne by another party, such as Party D, leading to inefficient outcomes. A typical example is in the context of insurance contracts – a person who enters into an auto insurance contract may be less careful in her driving because she is covered by insurance and the losses from her carelessness would be borne by the insurance company instead.[57]

Box 10: OCBC phishing scams in 2021 and moral hazard[58]

The issue of moral hazard featured strongly during the 2021 OCBC phishing scams incident. In an interview with Helen Wong, CEO of OCBC, it was shared that the OCBC team had to consider the problem of moral hazard before announcing that OCBC would provide customers with goodwill payouts for the scammed amount. OCBC was concerned whether such a move would result in customers being complacent about cybersecurity risks in the future, with the expectation that the customers would be compensated if they fell victim to such scams. OCBC was also concerned that scammers would be incentivised to target Singapore banks if they expected that banks would back their customers.[59]

In addition, there were also concerns of moral hazard in relation to OCBC's response, in particular whether the banks had lapsed in how they responded to the scam and whether the banks had taken reasonable steps to protect the interests of clients.[60] There were media reports about victims being left on

[57] Duc V Trang, *Architecture of Deals: Strategies for Transactional Lawyering* (Singapore, Academy Publishing, 2019) at [11.4] ("Trang").
[58] "What is cyber insurance", *supra* n 56.
[59] Candice Cai, "OCBC phishing attacks were 'fast and furious' and 'well-strategised', says group CEO", *AsiaOne* (23 January 2022) <*https://www.asiaone.com/singapore/ocbc-phishing-attacks-were-fast-and-furious-and-well-strategised-says-group-ceo-helen-wong*> (accessed 14 October 2023).
[60] "Did OCBC set a precedent", *supra* n 54.

hold on the bank's hotlines for extended periods of time and were unable to connect to the bank to stop the unauthorised transactions.[61] In addition, OCBC had picked up in early December signs of such phishing scams. Although various actions had been taken to stem the phishing scam, it was noted by Lawrence Wong (then Minister for Finance and Deputy Chairman of the Monetary Authority of Singapore) that OCBC "should however have responded faster and more robustly at the first sign of the scams".[62] Some victims pointed out that OCBC had previously sent marketing messages with links via SMS, and that they had been conditioned to click on such links. Given that OCBC was aware that the SMS channel could be compromised, some victims argued that OCBC should have made efforts to secure or disable such a channel.[63]

50. Given the above moral hazard considerations, the Subcommittee is of the view that it is necessary to specify the duties of each party to the transaction chain to prevent risks of unauthorised use from arising *ex ante* and mitigate losses arising from such unauthorised use *ex post*.

51. In determining what might be the appropriate duties, the Subcommittee is mindful that this requires consideration of the following (adapting from the seminal decision in *BNJ v SMRT* [2014] 2 SLR 7 at [55]):

    a. Magnitude and likelihood of harm that may result from the risk eventuating; and

    b. Trade-offs between the benefits and costs of any proposed precautions.

52. With respect to the magnitude and likelihood of harm, the Subcommittee is unaware of any publicly available study pertaining to unauthorised transactions and Digital Identities in Singapore. That being said, while the probability itself is uncertain, the Subcommittee is of the view that the magnitude of the harm itself is often catastrophic for users of Digital Identities (such as users of Singpass and other bank Digital Identities). For example, many victims of the 2021 OCBC scams had lost their entire life savings as a result of the scam.[64] Even if the probability of such

[61] Kenny Chee & Dominic Low, "How SMS Phishing scams have affected OCBC customers and put text messaging security in focus", *The Straits Times* (22 January 2022) <*https://www.straitstimes.com/tech/tech-news/how-sms-phishing-scams-have-affected-ocbc-customers-and-put-text-messaging-security-in-focus*> (accessed 14 October 2023).
[62] Lawrence Wong, Minister for Finance and Deputy Chairman of the Monetary Authority of Singapore, "Bolstering the Security of Digital Banking", Ministerial Statement (15 Februrary 2022) <*https://www.mas.gov.sg/news/speeches/2022/bolstering-the-security-of-digital-banking---ministerial-statement*> (accessed 14 October 2023).
[63] Low Jia Ying, "OCBC S'pore scam victims, many who lost life savings, slam bank for underwhelming response", *Mothership* (14 January 2022) <*https://mothership.sg/2022/01/ocbc-scam-victims/*> (accessed 14 October 2023).
[64] *Ibid*.

unauthorised use is extremely rare, the catastrophic nature of such unauthorised use (that is, black swan events) clearly warrants parties to take *some steps* to prevent such risks from occurring and to mitigate losses arising from their occurrence.

53. On the benefits and costs of any proposed precautions, the Subcommittee is mindful of differences in the parties' abilities to prevent risks from occurring and mitigate losses arising from unauthorised use of Digital Identities. In particular, there may be cognitive biases and limitations on individuals which makes certain precautions onerous or practically ineffective, in contrast with sophisticated businesses who rely on such Digital Identities.

54. The Subcommittee also notes a final point as to how such duties are specified: whether specific rules should be utilised, or a broad standard of care should be imposed instead on each party to the transaction chain. The use of rules (which are more specific and detailed) provides for more precision, although there may be concerns as to whether such rules could be over or under-inclusive in addressing moral hazard concerns. In contrast, a broad standard could be specified (for example, parties must take reasonable care) as opposed to imposing specific rules, which leaves the adjudicator the task of determining the content of what is permissible and the factual issues at hand.[65] This, however, comes at the expense of certainty and may result in *ex post* transaction costs (such as the costs of litigation).

55. A possible middle ground would be to establish as many practices identified below as specific rules, with a broader standard requiring parties to take "reasonable care" as a catch-all. Other identified practices not specified as rules could instead become relevant factors for an adjudicator's consideration as to whether the requisite standard of care was met. In line with this approach, the Subcommittee has sought to outline such practices as specific rules where possible, but notes that these could be utilised as factors under a broad standard as well.

B. OBLIGATIONS OF USERS

1. Risk prevention

56. The Subcommittee notes that there are three broad areas in which Users could prevent risks of Digital Identity's unauthorised use.

57. The first area relates to steps which seek to *ensure that passwords are sufficiently robust and safeguarded*. One key Authenticator which is relied on in the Id(Entity) Authentication is the text-based password. Upon presentation of the relevant Authenticators for the purposes of Id(Entity) Authentication, the user will be authorised to enter into Legal Transactions. For example, Singpass uses the public key infrastructure ("**PKI**") for its Sign with Singpass service. The private key may be used to create a digital

[65] Trang, *supra* n 57, at [14.9].

signature, or to decrypt an electronic record that was encrypted with the corresponding public key. The associated public key can be used to verify a digital signature created with the corresponding private key, or to encrypt an electronic record such that it may be decrypted with the corresponding private key.[66] *However, the entire infrastructure is only as strong as the user's Singpass Authenticators (including the password) which must be presented for Id(Entity) Authentication before Sign with Singpass can be used*.[67]

58. Specific obligations are often imposed on Users in relation to their passwords. Common ones include requiring Users:[68]

    a. Not to share their passwords with others;

    b. Not to record down passwords in an insecure manner; or

    c. To periodically change passwords.

    Digital Identity providers may also require passwords to be sufficiently complex, before services are provided to the legal persons.

59. The benefits of imposing these obligations, however, remain to be seen. A few important points can be noted:

    a. Practices previously thought to increase security have instead been found to do the opposite.[69] Increasing password complexity by forcing upper and lower-case characters, numbers, and special characters in passwords is common practice. However, users tend to respond to such requirements very predictably (such as by using "Password1!" instead of "password") and thus do not significantly strengthen their passwords. Furthermore, this introduces additional vulnerabilities by reducing memorability, increasing the likelihood that they are written down in an insecure manner or forgotten.[70]

    b. There is frequently a trade-off between the memorability and strength of passwords.[71] In an empirical study of leaked data of 6 million Chinese Software Developer Network website user accounts, 83% of users used some meaningful data (e.g., birthday) in choosing their password. This renders it easier to remember,

---

[66] Singpass Terms of Use, *supra* n 51, at Clause 1.2.2, Annex 5.

[67] Stephen Mason & Daniel Seng, *Electronic Evidence and Electronic Signatures* (London, Institute of Advanced Legal Studies, 2021) at para 7.259

[68] See for example the Monetary Authority of Singapore, *E-Payments User Protection Guidelines* (5 September 2020) at para 3.4 – 3.5.

[69] Bonneau et al., "Passwords and the evolution of imperfect authentication" (2015) 58:7 Communications of the ACM 78.

[70] National Institute of Standards and Technology, "NIST Special Publication 800-63B: Digital Identity Guidelines" (updated 2 March 2020) at Appendix A.3, "Complexity".

[71] Richard Shay et al., "Designing Password Policies for Strength and Usability" (2016) 18:4 ACM Transactions on Information and System Security 13:1.

but also significantly reduces the number of guesses required for hackers to crack the password.[72]

c. Regular password expiry is no longer seen as an effective security policy, as the repeated changing of passwords that must conform to a certain standard ultimately creates more vulnerabilities than it resolves. For example, users are likely to choose new passwords with only minor variations of the old passwords. Stolen passwords are generally exploited immediately. Resetting passwords also gives no information about whether a compromise had occurred, and attackers with access to the Digital Identity would also receive requests to reset the password.[73] The Personal Data Protection Commission recommended regular password changes in 2017,[74] but not in 2021.[75]

d. Password sharing is likely to be a common practice by the older generation or those who may be less technologically literate. These individuals often have no choice but to rely on others in order to utilise their Digital Identities for their day-to-day transactions.

60. The second area relates to scam prevention by Users. As can be seen from the earlier examples,[76] many instances of unauthorised transactions from Digital Identities arose because Users fell victim to scams. Unlike password policies above, it may be difficult to specify exactly what the User must do before that User is regarded as blameworthy for the following reasons:

a. First, Users are not a monolithic class. There may be sophisticated individuals who are technologically savvy and are aware of the risks associated with the use of Digital Identity. On the other hand, there are also those who may be less so and are unaware of such risks.

b. Second, the types of scams are varied and exploit different vulnerabilities. For example, the 2021 OCBC phishing scams exploited customers' concerns that their accounts could have been compromised, playing on customers' loss aversion. In contrast, other scams may rely on the greed of individuals (such as luring individuals with attractive offers and promotions), enticing such

---

[72] Chao Shen et al., "User practice in password security: An empirical study of real-life passwords in the wild" (2016) 61 Computers & Security 130.

[73] UK National Cyber Security Centre website, "Password policy: updating your approach" <*https://www.ncsc.gov.uk/collection/passwords/updating-your-approach*> (accessed 18 June 2023).

[74] Personal Data Protection Commission Singapore, *Guide to Securing Personal Data in Electronic Medium*, published on 8 May 2015, and revised on 20 January 2017. Cited in Lovebonito Singapore Pte. Ltd. [2022] SGPDPC 3 at [20].

[75] SG Digital Office & Personal Data Protection Commission Singapore, *Guide to Data Protection Practices for ICT Systems* (2021) ("*Guide to Data Protection Practices*")

[76] See para [36] and Box 7. above.

individuals to download malware.[77] The blameworthiness of the individuals and the steps required to be taken would be incident-specific. Specifying a general rule is unlikely to be possible as they may become under or over-inclusive.[78]

61. One possible solution might be that a standard could be specified instead. This allows the adjudicator to adjust for factors such as the vulnerability of the User, the type of scam involved and the blameworthiness of the User.[79] For example, under regulation 77(3)(b) of the UK's Payment Services Regulation 2017 ("**PSR**") a payment service user who has, with gross negligence, failed to comply with their obligations under regulation 72 of the PSR regarding the use of the payment instrument and keeping safe of personalised security credentials, will be liable for all losses incurred. Regulation 72 of the PSR requires the payment service user to take all "reasonable steps to keep safe personalised security credentials relating to a payment instrument or an account information service." Facilitating this approach might be that Digital Identity providers could provide warnings to Users, putting them on notice of potential risks, and a failure to have regard to such warnings could go towards establishing breach.[80]

62. A second solution might be to establish certain classes of claims for which the losses should be borne by the User, without having to specify any duties and establishing their breach (that is, a strict liability approach). For example, Etiqa's Personal Cyber Insurance broadly excludes from its cover losses arising from confidence scams that involve feigned intentions towards a User (such as romantic intentions), gaining the User's confidence or affection and using such goodwill to commit fraud.[81] Such an approach can be taken for specific instances where the risk of under-inclusiveness is likely to be low (that is, a person who fell victim to such scams would typically be negligent).

63. The last area relates to Users taking steps to maintain the security of their electronic devices. The following are three possible obligations:

    a. Users are required to update their device's software or operating systems. For example, the E-Payments Guidelines impose on users the duty to update their device operating systems and browsers to the latest available version.[82] The obligation to keep

---

[77] Kurt Ganapathy, "Worried about falling victim to an Android malware scam? Look out for these red flags", *Channel NewsAsia* (15 August 2023) <*https://www.channelnewsasia.com/singapore/android-malware-scam-tactics-install-app-spf-csa-advisory-3700971*> (accessed 14 October 2023).
[78] Trang, *supra* n 57, at [14.9].
[79] *Id*, at [14.5].
[80] Payment Systems Regulator, *Authorised push payment scams, the consumer standard of caution (Consultation Paper)* (CP23/7, 2023) at [3.2] in the context of authorised push payment scams.
[81] Etiqa, Personal Cyber Insurance at Clause 3.4 <*https://www.etiqa.com.sg/wp-content/uploads/2020/07/Etiqa_Policy_Wording_Tiq-Personal-Cyber-UTD-28052020.pdf*> (accessed 14 October 2023).
[82] Monetary Authority of Singapore, *E-Payments User Protection Guidelines* (5 September 2020) at para 3.6 ("*E-Payments User Protection Guidelines*").

systems updated is also reported to be a standard term in cyber-security insurance policies.[83]

b. Users are also required to install and maintain antivirus software on their devices.[84]

c. Users should only download and install applications from official application stores, and should not install applications from unknown sources.[85]

64. The Subcommittee notes that compliance with the obligations is unlikely to impose significant costs on Users. In many situations, updates are often pushed to Users by manufacturers of devices and software, requiring only that the User consent before updating takes place. As for antivirus, most modern Windows and Apple computers, as well as Android and Apple smartphones would come with built-in antivirus software that only requires periodic updating.[86] Lastly, most operating systems for devices would prompt Users when an application comes from a suspicious source, thereby putting Users on notice of potential risks. In such situations, imposing losses on Users for breaches of these obligations would ensure Users are sufficiently incentivised to ensure their devices' security.

2. Loss mitigation

65. With regard to loss mitigation, the Subcommittee notes that there are also three broad areas relevant to Users.

66. First, Users could be imposed with an obligation to verify the Legal Transaction history of their Digital Identities, when such history is made available to Users. This duty is analogous to a duty to verify bank statements – the terms and conditions of standard banking documentation often incorporate conclusive evidence clauses.

67. Such clauses impose an obligation on the User to verify their bank statements and notify the bank of forgery or unauthorised transactions in a stipulated period. A failure to notify such forgery or unauthorised transactions may allow a bank to treat the statement as conclusive evidence of its contents. The Subcommittee notes that such clauses have generally been upheld in the Singapore Courts,[87] save for when such clauses purport to

---

[83] Gravity Risk Services, "Will my cyber insurance pay out?" <*https://www.gravityriskservices.co.uk/will-my-cyber-insurance-pay-out/*> (accessed 21 June 2023)
[84] *E-Payments User Protection Guidelines*, *supra* n 82, at para 3.6.
[85] Singapore Police Force & Cyber Security Agency of Singapore, "Joint Advisory on the Dangers of Downloading Applications from Third Party or Dubious Sites" at [4a] <*https://www.police.gov.sg/media-room/news/20230411_joint_adv_on_the_dangers_of_downloading_apps_from_third_part_or_dubious_sites*> (accessed 14 October 2023).
[86] Australian Signals Directorate, Government of Australia, "Antivirus software" <*https://www.cyber.gov.au/protect-yourself/securing-your-devices/how-secure-your-device/antivirus-software*> (accessed 14 October 2023).
[87] See *Jiang Ou, supra* n 50 at [73]-[91] for a survey of the relevant case law.

exclude liability for fraud of the banks' employees (which would run afoul of the reasonableness test under S11 of the Unfair Contract Terms Act 1994).[88]

68. The Subcommittee notes that such an obligation is unlikely to be onerous in light of modern practices. It is now common practice for banks to require customers to receive push notifications on their smartphones, and immediately deliver notifications of outgoing transactions above a certain threshold whenever they occur. Push notifications provide immediate feedback of a transaction, so the user would naturally know if the transaction was unauthorised. As such, Users will be able to discover within a short period of time of any unauthorised transactions entered into with their Digital Identity.

69. Second, Users could be required to take reasonable steps to notify the Digital Identity provider of any security breaches (such as the loss or compromise of any Authenticator) pertaining to their Digital Identity which they are aware of, as well as any relying party which may be affected. For example, in the context of bank cards, a User must notify the card provider "as soon as reasonably practicable after becoming aware that [their] card has been lost or stolen".[89] There does not appear to be any concern about such an obligation being onerous and as seen from the 2021 OCBC phishing scam, many Users would do so on their own initiative as well.[90]

70. Third, Users could be required to take independent remedial actions, for example triggering a "kill switch" which immediately freezes a Digital Identity. Following the 2021 OCBC phishing scam, OCBC has provided customers with a "kill switch" that allows users to immediately freeze all their bank accounts without having to go through a representative of the bank.[91] Similar kill switches have also been provided by DBS[92] and UOB.[93]

71. The Subcommittee notes that this differs from informing the bank of security breaches or verifying transaction history, as it places the burden of assessing the transactions and freezing the account upon the independently-acting user. Such a kill switch could also be implemented for digital identities. It would be possible to require users to reasonably use the tools made available to them to mitigate losses. However, the Subcommittee notes that it is unclear whether mandating such an obligation as a specific rule will be practical or effective, considering the wide spectrum of technical and

---

[88] *Id,* at [105]-[122].

[89] The Association of Banks Singapore, *Code of Practice for Banks - Credit Cards* (revised 2 July 2020) at para 5(a).

[90] See para [49] and Box 10. above.

[91] OCBC Bank, "OCBC Bank rolls out emergency kill switch so customers can freeze all accounts if scammed" (16 February 2022) <*https://www.ocbc.com/group/media/release/2022/ocbc-rolls-out-emergency-kill-switch.page*> (accessed 25 June 2023)

[92] DBS website, "Safety Switch" <*https://www.dbs.com.sg/personal/support/bank-ssb-safety-switch.html*> (accessed 14 October 2023).

[93] UOB website, "How you can protect yourself" <*https://www.uob.com.sg/personal/digital-banking/pib/security/how-you-can-protect-yourself.page*> (accessed 14 October 2023).

financial literacy amongst users. It may be better instead to regard whether such steps are taken as a factor in assessing if any broad standard imposed on Users was breached.

Questions for User Obligations and Secondary Fault Liability

1. Are there practices, perspectives or policy considerations which are not outlined above which the Subcommittee should consider in determining the obligations of a User for the purposes of Secondary Fault Liability?

2. Are there any obligations outlined above which should not be imposed on a User?

3. Are there any obligations not outlined above, but should be imposed on a User?

4. Are the obligations outlined above sufficiently clear and precise, and if not, how can they be improved?

C. OBLIGATIONS OF DIGITAL IDENTITY PROVIDER

1. Risk prevention

72. The Subcommittee notes it is likely to be difficult to develop specific rules in this area given the rapid pace of technological and fraud developments. As such, the Subcommittee is preliminarily of the view that obligations should be imposed on the Digital Identity provider based on a broad standard such as reasonable care instead. Issues such as what the best practices are at a given time, and the costs associated can be considered by the relevant adjudicator on a case-by-case basis. With regard to risk protection, the Subcommittee notes three areas of concern.

73. First, the Digital Identity providers dictate the (Id)Entity Authentication process and specify what Authenticators are relevant. As such, they play an important role in ensuring that access controls implemented are sufficiently secure and ought to take reasonable care in designing their systems. Some possible factors in determining whether the Digital Identity provider has breached its duty to take reasonable care may include:

    a. Whether the Digital Identity provider had utilised Multi-Factor Authentication as part of its system. For example, it is now standard market practice to require the use of Authenticators such as passwords, in combination with other Authenticators such as one-time passwords. More recently, facial recognition has been introduced as a log-in procedure for vulnerable members of the CPF using Singpass (which includes those aged 55 and above and

who are using Android phones), as a response to the 2023 CPF malware scams.[94] Such a feature was introduced as malware could compromise the other Authenticators such as passwords and one-time passwords sent to the CPF member's phone, and biometric verification became the only safeguard remaining that was viable; and

b. Whether the Digital Identity provider had implemented the latest best practices and anti-fraud measures with its Authentication process. This would require the Digital Identity provider to periodically review its Authentication processes and make adjustments accordingly to emerging risks. For example, deepfake technology has been becoming increasingly sophisticated – deepfake technology involves the use of neural networks to replicate the target's face onto another person, which may impede the effectiveness of facial recognition technology.[95] As a result, the use of facial recognition should be accompanied with the relevant anti-spoofing technology.[96] In this regard, the Subcommittee notes that Singpass' Identiface utilises Presentation Attack Detection technology (which uses illumination techniques such as flashing coloured lights) to detect spoofing attempts.[97]

74. Second, Digital Identity providers should be required to conduct periodic security penetration testing with reasonable care. Penetration testing refers to the employment of methods to identify security vulnerabilities and remedy these vulnerabilities before security breaches actually occur. Penetration testing encompasses assessing vulnerabilities from the perspective of "hardware, software and people", and is performed by "simulating an unauthorized user attacking the system".[98] This allows the Digital Identity provider to "fine-tune and test configuration changes or patches to proactively eliminate identified risk".[99] Penetration testing assists digital identity providers to keep up with the rapid advancement of technology in spoofing and other potential attack vectors.

75. The Subcommittee notes that the importance of penetration testing has been stressed in numerous regulations:

---

[94] "New Singpass face-verification feature for CPF log-in to protect the vulnerable against malware scams", *Channel NewsAsia* (29 June 2023) <*https://www.channelnewsasia.com/singapore/cpf-singpass-face-verification-log-malware-scam-protection-govtech-police-3594076*> (accessed 14 October 2023).

[95] Pavel Korshunov and Sébastien Marcel, "Deepfake: a New Threat to Face Recognition? Assessment and Detection" (2018) arXiv 1 at p 4, where the authors found that certain facial recognition algorithms that were based on VGG or Facenet failed to detect the use of deepfakes up to a 95.00% equal error rate.

[96] *Ibid*.

[97] Singpass website, FAQ, Q5, <*https://api.singpass.gov.sg/library/identiface/business/faq*> (accessed 14 October 2023).

[98] Aileen G Bacudio et al, "An Overview of Penetration Testing" (2011) 3 International Journal of Network Security and its Applications 19 at p 19.

[99] *Id,* at p 20.

a. In the area of data protection, the Personal Data Protection Commission of Singapore has emphasised that penetration testing or other forms of vulnerability assessment should be conducted on a website prior to its launch and on a periodic basis.[100] It has been observed that "the Singaporean PDPC mentioned penetration testing as a requisite security control in over 60 enforcement decisions for violations of the PDPA (Personal Data Protection Act) in Singapore, leaving no doubt about its perceptions of penetration testing in the security context".[101]

b. Similarly, the Cyber Security Agency of Singapore has stressed the need for penetration testing in relation to critical information infrastructure, mandating for penetration tests annually or biennially and when there are any major systems changes to the critical information infrastructure.[102]

c. Financial institutions are also required to conduct penetration testing to evaluate their cyber security defences at least once annually or when there are major changes or updates to the system.[103]

76. Third, ancillary to the conduct of penetration tests is the need to patch out vulnerabilities when discovered. A digital identity provider should have a duty to take reasonable care in patching out such vulnerabilities to ensure that its software is up to date.

77. Similar to the duty to conduct penetration testing, the requirement to patch out vulnerabilities and to maintain the most recent software has been emphasised in numerous regulations as well:

a. In the area of data protection, the PDPC has "consistently advised organisations on the importance of applying software patches".[104] In *Fortytwo Pte Ltd*[105], the Personal Data Protection Commission found that the company's failure to implement four patches which were released by Adobe to "address several high severity risk issues and critical bugs, including the injection of malicious code", was a breach of section 24(a) of the PDPA which

---

[100] See *Guide to Data Protection Practices*, *supra* n 75, at p 21.
[101] Ilia Kolochenko, "Penetration testing in the modern regulatory and legal landscape", *Security* (22 June 2021) <*https://www.securitymagazine.com/articles/95477-penetration-testing-in-the-modern-regulatory-and-legal-landscape*> (accessed 14 October 2023).
[102] Cyber Security Agency of Singapore, *Cybersecurity Code of Practice for Critical Information Infrastructure – Second Edition* (4 July 2022) at p 37 ("*Cybersecurity Code of Practice*").
[103] Monetary Authority of Singapore, *Technology Risk Management Guidelines* (January 2021) at pp 45-46 ("*Technology Risk Management Guidelines*"); Association of Banks in Singapore, *Penetration Testing Guidelines for the Financial Industry in Singapore* (31 July 2015).
[104] *Fortytwo Pte. Ltd.* [2023] SGPDPC 3 at para 9 ("*Fortytwo Pte. Ltd.*"). See also *Guide to Data Protection Practices*, *supra* n 73, at p 27.
[105] *Fortytwo Pte. Ltd.*, *supra* n 104.

requires organisations to protect personal data in its possession by making reasonable security arrangements.[106]

b. The CSA likewise has underscored the importance "for organisations to monitor for new vulnerabilities and their corresponding security patches, and to develop procedures to apply the security patches promptly".[107]

c. Financial institutions must also establish a patch management process to fix security vulnerabilities and software bugs.[108] This patch management process must consider the severity of the vulnerability and must be "commensurate with (a) the criticality of the affected systems (b) the risk that the vulnerability poses".[109]

2. Loss mitigation

78. With regard to loss mitigation, the Subcommittee has considered three broad areas relevant to Digital Identity providers.

79. First, Digital Identity providers should have an obligation to notify the Users about transactions carried out using the digital identity. This follows as a corollary to Users' duties to verify and identify any unauthorised transactions, and would allow Users to freeze or suspend their Digital Identity thereby minimise the resulting losses.

80. The Subcommittee notes that such an obligation is commonly imposed in practice. For example, such duties have been imposed on financial institutions – under the E-Payment User Protection Guidelines, a financial institution must provide transaction notifications to each account holder – while the transaction notifications are mandatory for outgoing transactions, it is only encouraged for incoming transactions.[110] The transaction notifications must meet certain minimum requirements – for instance, the notifications must contain information that would allow the account holder to identify the related account, recipient, transaction amount, time, date and type.[111] Nonetheless, the User may opt out from receiving such transaction notifications.[112]

---

[106] *Id,* at para 11.
[107] *Cybersecurity Code of Practice*, *supra* n 102, at p 33.
[108] *Technology Risk Management Guidelines*, 103 at p 24. See e.g. MAS Notice 655, *Notice on Cyber Hygiene* in relation to Banks at para 4.2; MAS Notice CMG-N03, *Notice on Cyber Hygiene* in relation to relevant capital markets entities at para 4.2.
[109] Monetary Authority of Singapore, *Frequently Asked Questions: Notice on Cyber Hygiene* at para A3.
[110] Monetary Authority of Singapore, *E-Payment User Protection Guidelines* (28 September 2018) at paras 4.4, 4.7.
[111] *Id,* at para 4.4.
[112] *Id*, at para 4.5.

81. An obligation to notify breaches has also been imposed on certification authorities of digital signatures. For instance, a certification authority must use reasonable efforts to notify users that may be affected by a material and adverse breach in its security.[113] A certification authority is also required to notify the user within a reasonable period of time of any fact known to the certification authority that significantly affects the validity or reliability of the certification.[114]

82. Second, Digital Identity providers should provide Users with kill switches, allowing a User to terminate his or her Digital Identity immediately once he or she is aware that it has been compromised. As noted above, such kill switches have been implemented by local banks such as OCBC, DBS and UOB following the 2021 OCBC phishing scam.[115] Similarly, certification authorities of digital signatures must suspend or revoke the digital certificate as soon as possible after receiving a request from a user.[116]

83. Last, a Digital Identity provider should be obliged to suspend the Digital Identity of a User upon discovery that such Digital Identity was compromised, and to inform any affected User and relying party of such compromise. This is because there may be some delay for a User to trigger the kill switch or to make the request for suspension, and the fraudster can potentially misuse the Digital Identity in that short amount of time. For example, while a certification authority *may* suspend a certificate if it has reasonable grounds to believe that the certificate is unreliable, it must conduct investigations into the reliability of the certificate.[117] Upon confirming that the private key or trusted system is compromised, and reliability is materially affected, the certification authority must suspend the certificate.[118]

Questions for Digital Identity provider Obligations and Secondary Fault Liability

1. Are there practices, perspectives or policy considerations which are not outlined above which the Subcommittee should consider in determining the obligations of a Digital Identity provider for the purposes of Secondary Fault Liability?

2. Are there any obligations outlined above which should not be imposed on a Digital Identity provider?

[113] Rule 13(2) of the Third Schedule to the Electronic Transactions Act 2010 ("ETA").
[114] Reg 16 of the Electronic Transactions (Certification Authority) Regulations 2010 ("ET(CA) Regs").
[115] See para [69] above.
[116] Third Schedule to the ETA, *supra* n 113, Rules 16 and 17.
[117] ET(CA) Regs, *supra* n 114, Reg 18(4).
[118] Third Schedule to the ETA, *supra* n 113, Rule 18.

3. Are there any obligations not outlined above, but should be imposed on a Digital Identity provider?

4. Are the obligations outlined above sufficiently clear and precise, and if not, how can they be improved?

D. OBLIGATIONS OF RELYING PARTY

1. Risk prevention

84. Since the relying party directly interacts with the fraudster in the event of a Digital Identity being compromised, the relying party may be in a position to detect any anomalous behaviour or indications of fraud. As such, the Subcommittee is preliminarily of the view that relying parties should have an obligation to ***take reasonable steps to detect suspicious transactions*** arising from the use of Digital Identities.

85. The Subcommittee notes it is likely to be difficult to develop specific rules in this area. The relying party is not a monolithic class and may have varying levels of sophistication, financial capability or technical ability to prevent risks of unauthorised use. As such, these obligations should be imposed on the relying party based on a broad standard such as reasonable care instead, allowing an adjudicator to adopt a fact-specific approach to determine each case.

86. In this regard, the Subcommittee notes that where the relying party is more sophisticated, and has the financial capability and the technical ability to prevent unauthorised use, more would be expected of such relying parties. Possible examples of such relying parties include banks and financial institutions and companies operating large e-commerce or online-shopping platforms. Such relying parties would have the resources to establish machine learning algorithms and transaction surveillance analysts[119] to detect fraudulent transactions, and would require a large historical dataset in terms of "recent and historical data and outcomes"[120] to develop models that can detect suspicious transactions.

[119] Tobias Knuth & Dennis C. Ahrholdt, "Consumer Fraud in Online Shopping: Detecting Risk Indicators through Data Mining" 26 International Journal of Electronic Commerce 388 at 398

[120] Andrew Tarantola, "Hitting the Books: How Southeast Asia's largest bank use AI to fight financial fraud", *Engadget* (25 September 2022) <*https://www.engadget.com/hitting-the-books-working-with-ai-davenport-miller-mit-press-150016191.html*> (accessed 14 October 2023).

2. Loss mitigation

87. A relying party should, upon being notified that a relevant Digital Identity has been compromised, be obliged to take reasonable steps to bring any transactions entered into in reliance of the Digital Identity to an end.

88. The Subcommittee notes that a parallel may be drawn to the doctrine of mitigation under contract law: an aggrieved party must take all reasonable steps to mitigate the loss consequent on the defaulting party's breach, and cannot recover damages for any loss which it could have avoided but failed to avoid due to its own unreasonable action or inaction.[121] The aggrieved party may recover expenses reasonably incurred in the course of taking mitigation measures.[122] Such an approach would require an adjudicator to evaluate the case at hand in order to arrive at a commercially just determination.[123]

89. How would such a duty to mitigate losses apply in the context of compromised Digital Identities? Consider the situation where an online merchant relied on a contract for the sale of custom furniture entered into with a compromised Digital Identity, and had entered into further transactions such as purchasing material and arrangement of third-party shipping. The online merchant would be required to take steps to cancel such further transactions where possible. While the merchant might be required to pay a default fee, the Subcommittee is of the view that such fees could be recovered from the User (if imposed with the Primary No-Fault Liability) as expenses reasonably incurred in the course of taking mitigation measures.

Questions for relying party Obligations and Secondary Fault Liability

1. Are there practices, perspectives or policy considerations which are not outlined above which the Subcommittee should consider in determining the obligations of a relying party for the purposes of Secondary Fault Liability?

2. Are there any obligations outlined above which should not be imposed on a relying party?

3. Are there any obligations not outlined above, but should be imposed on a relying party?

4. Are the obligations outlined above sufficiently clear and precise, and if not, how can they be improved?

[121] *The "Asia Star"* [2010] 2 SLR 1154 at [24].
[122] *Id*, at [24].
[123] *Id*, at [32].

ANNEX: CONSOLIDATED LIST OF QUESTIONS

Questions for Digital Identities and Legal Transactions

1. Are there perspectives, policy considerations or market practices which are not outlined above which the Subcommittee should consider in defining "Digital Identity" for Legal Transactions?

2. What are some other features which the Subcommittee should consider incorporating in the concept of Digital Identity?

3. What are some features which the Subcommittee has identified that should not be incorporated in the concept of Digital Identity?

Questions for unauthorised transactions, liability framework and need for reform

1. Are there perspectives or policy considerations which are not outlined above which the Subcommittee should consider in developing the liability framework for unauthorised transactions?

2. Is the classification of Primary No-Fault Liability and Secondary Fault Liability appropriate?

3. Is law reform necessary to address the aforementioned issues?

Questions for Primary No-Fault Liability

1. Are there perspectives or policy considerations which are not outlined above which the Subcommittee should consider in recommending on whom the Primary No-Fault Liability should be allocated?

2. Given the policy considerations, as between the legal person(s) linked to the Digital Identity and the relying counterparties, who should be allocated the Primary No-Fault Liability?

3. Should there be mandatory insurance to compensate for losses that may arise from the unauthorised use of Digital Identities?

Questions for User Obligations and Secondary Fault Liability

1. Are there practices, perspectives or policy considerations which are not outlined above which the Subcommittee should consider in determining the obligations of a User for the purposes of Secondary Fault Liability?

2. Are there any obligations outlined above which should not be imposed on a User?

3. Are there any obligations not outlined above, but should be imposed on a User?

4. Are the obligations outlined above sufficiently clear and precise, and if not, how can they be improved?

Questions for Digital Identity provider Obligations and Secondary Fault Liability

1. Are there practices, perspectives or policy considerations which are not outlined above which the Subcommittee should consider in determining the obligations of a Digital Identity provider for the purposes of Secondary Fault Liability?

2. Are there any obligations outlined above which should not be imposed on a Digital Identity provider?

3. Are there any obligations not outlined above, but should be imposed on a Digital Identity provider?

4. Are the obligations outlined above sufficiently clear and precise, and if not, how can they be improved?

Questions for relying party Obligations and Secondary Fault Liability

1. Are there practices, perspectives or policy considerations which are not outlined above which the Subcommittee should consider in determining the obligations of a relying party for the purposes of Secondary Fault Liability?

2. Are there any obligations outlined above which should not be imposed on a relying party?

3. Are there any obligations not outlined above, but should be imposed on a relying party?

4. Are the obligations outlined above sufficiently clear and precise, and if not, how can they be improved?