Threats and cybercrime in the Digital Identity space

DGX Digital Identity Working Group – 2023

Table of Contents

DGX Digital Identity Working Group – 2023

1. Introduction

About the DGX-DIWG

The Digital Government Exchange (DGX) Digital Identity Working Group (DIWG) was established in 2020 by representatives of the DGX international group. The purpose of the DIWG is to share experiences and opportunities for the use of digital identity initiatives, initially with a focus on the response to and recovery from the impacts of COVID-19 on governments and people. It also provides an opportunity to collaborate and drive progress on mutual recognition and interoperability of digital identities between member countries.

The current membership for the DIWG was formalised in February 2023 and is chaired by Singapore's Government Technology Agency, with members from Australia, Germany, Israel, New Zealand, and Singapore. It is represented by many leading governments with digital identity initiatives.

In 2023, the working group aims to build the partnership between the DIWG to have active collaboration and knowledge sharing regarding the trend of scams and the effort taken to combat scams.

2. Working Group Approach

The COVID-19 pandemic had expedited widespread digital adoption globally. In recent years, the rapid digital transformation witnessed has undeniably brought forth greater connectivity and convenience. However, as digital dependency and adoption increase, nations are also exposed to unprecedented cyber risks and vulnerabilities. Threat landscape is complex and the threats evolve continuously. Through the months of discussion, the DIWG had identified common digital threats that are commonly faced by various countries in the work group in Table 1.

Table 1: Threat Landscape Overview

Cybersecurity	Cybercrime	ID Theft

Ransomware:
• Motivated by financial gains
• Carried out by Advanced Persistent Threat (APTs)
	Scams:
	• Motivated by financial gains
	• Carried out by Criminals groups
	• Can be either:
	  ○ Knowingly disclosed
	  ○ Semi-knowingly disclosed
	  ○ Unknowingly disclosed
	• Enabled by:
		Impersonation scams involving Government Officials, Job Recruitment, and Romance:
		• Motivated by financial gains, and leverage over individuals / realistic social engineering.
		• Carried out by Advanced Persistent Threats (APTs)
		• Carried out via malware

	○ Poor business practices ○ Low or improper authentication	• Enabled by: ○ Poor business practices ○ Over-identification and collect of information. ○ Poor or absent binding ○ Poor user knowledge of identification practices

Among the three identified threat landscapes, the DIWG members noted the surge of cybercrimes such as phishing scams. In 2022, phishing was the highest reported cybercrime type, affecting at least 300,000 individuals globally[1]. Cybercriminals leverage creative tactics and exploit weak digital security measures to prey on unsuspecting victims. Often, these scammers seize control of the victim's digital identity and conduct fraudulent transactions.

Following OECD's definition, digital identity is a set of validated digital attributes and credentials that can be used to prove the unique identification of an individual[2]. An individual's digital identity enables transactions in the digital world and offers improved functionality for its user[3]. At its core, digital identity is about establishing trust between parties involved in a transaction. However, cybercrimes such as phishing compromises an individual's digital identity and often subject victims to financial loss and emotional distress[4], resulting in the loss of confidence in their digital identity. The proliferation of scam attempts not only generate substantial financial loss but ultimately threaten to tarnish citizens' trust in transacting digitally. As citizens' trust is the cornerstone for building a nation's digital identity, it is important for governments to come together and proactively find ways to combat cybercrimes and safeguard citizens' digital identity.

As such, the working group's objectives are to highlight the key approaches taken by member nations to combat cybercrimes and scams, identify existing gaps in current measures, and to explore innovative ways to increase digital identity protection.

[1] Global most frequently reported cybercrime by number of victims 2022 | Statista
[2] Recommendation of the Council on the Governance of Digital Identity | OECD
[3] Digital Identity on the Threshold of a Digital Identity Revolution | World Economic Forum
[4] Scam victims don't just get hit in the wallet; their mental health also suffers | The Straits Times

3. Findings on Common Scam Types

An international scan across DIWG members showed that most nations have high reported cases of phishing scams, e-commerce scams, and unauthorised transaction scams. The following aims to highlight common scam types reported, their resultant financial loss, and the modus operandi of these scams of member nations.

Table 2: Reported scams and financial losses by country level

Country	Population	Number of reported scams in 2022	Total financial loss to scams in 2022 (USD)	Top reported scam types
Australia	26.2 M	239,236	$368 M	1. Phishing 2. False billing 3. E-commerce scams
Germany	83.3 M	*<info unavailable>*	*<info unavailable>*	*<info unavailable>*
Israel	9.0 M	*<info unavailable>*	*<info unavailable>*	*<info unavailable>*
Singapore	5.6 M	31,728	$486 M	1. Phishing 2. Job Scams 3. E-commerce scams
New Zealand	5.2 M	8,160	$12 M	1. Phishing 2. Scams (e.g., loves scams, unauthorised transfers etc.)

Australia

In 2022, there were 239,236 cases of reported scams which resulted in a total of AUD$569 million lost to scams. Across all reports, 12% of individuals reported a financial loss and 27% reported the loss of personal information.

Among all scam types, phishing scams accounted for 31.2% of total scams and was the highest reported scam type. The 74,573 cases of phishing scams resulted in AUD$24.60 million of financial loss. This followed by 27,488 reports of false billing scams with AUD$24.83 million lost and 17,886 reports of e-commerce scams with AUD$9.24 million lost. Additionally, there were 16,212 reports of identity theft scams (6.8% of total scam types) which resulted in a financial loss of AUD$10.7 million[5].

In Australia, most scams are conducted via text messaging and phone calls. Scams conducted via phone calls also resulted in AUD$141 million lost which is the highest among all contact

[5] Targeting scams: report of the ACCC on scams activity 2022 | ACCC

modes. The breakdown of the various scam contact methods and their resultant financial loss can be seen from Figure 1 and Figure 2.

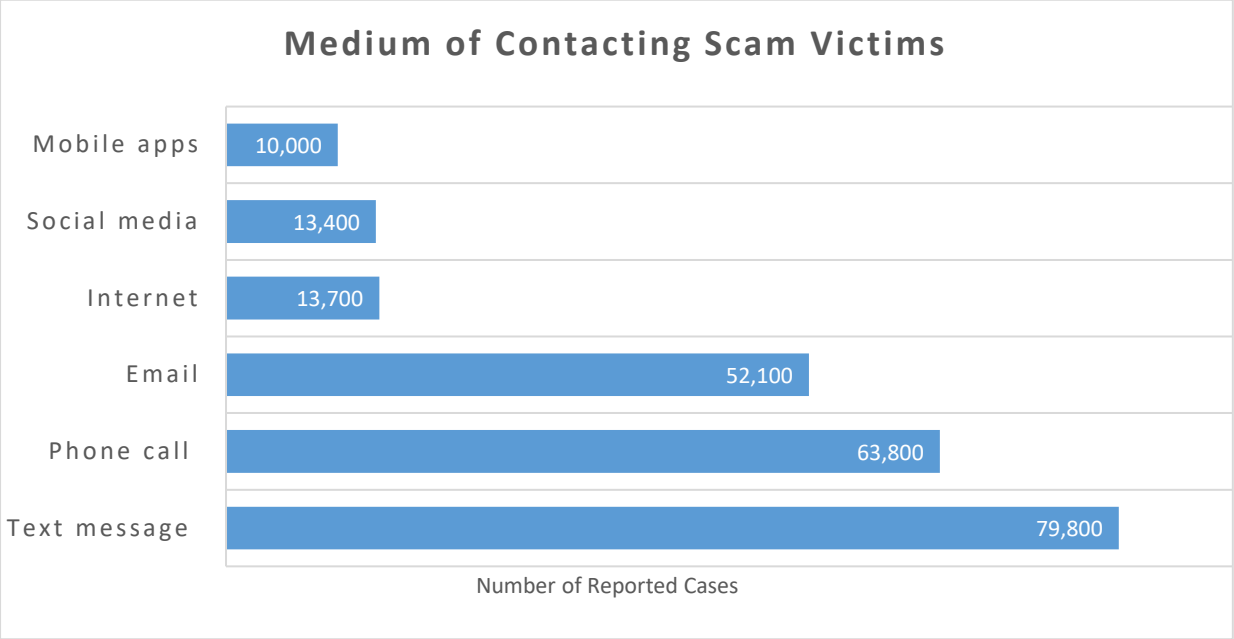

Figure 1: Medium of contacting scam victims (2022)

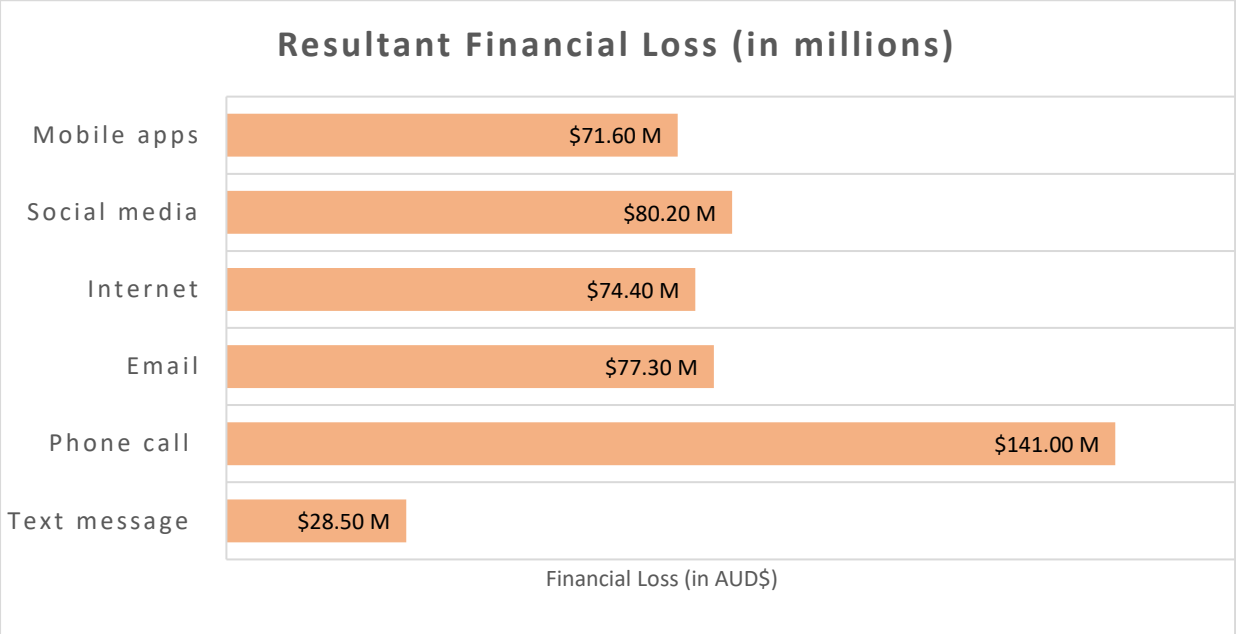

Figure 2: Resultant financial loss to medium of contact in Australia (2022)

Germany

Phishing scams are one of the most relevant hurdles when talking about secure digital identities. The European Union sets the common frame for digital identities in the EU. It includes the level of assurances[6], which distinguish digital identities according to their level of security:

1. *Low*: for instance, a username and password are used for self-registration on a webpage;
2. *Substantial*: for instance, a username and password are followed by a one-time password sent to your mobile phone;
3. *High*: for instance, enrolment is performed by digitally reading out a national ID Card.

Currently, eIDAS 2.0, a second version of this law is in discussion. The eIDAS 2.0 aims to set the regulatory framework for an EU-wide ID wallet. Security issues are being considered by all European security agencies, who form an expert group which informs the law-making process. Germany is represented by the Federal Office for Information Security[7].

The level of assurance applied by services directly correlates with the possibilities for fraud. While *low* levels of assurance in digital identities represent the most widespread solution for end users, they also incorporate the greatest risk for phishing or similar attacks. Digital identity cards on the other hand, which ensure a *high* level of assurance, only have a low market reach although their security level has proven to be almost impeccable.

Germany has one of the most restrictive understandings regarding data and information security. Especially in the public sector, citizens are usually required to identify on a *substantial* if not *high* level to access any service. Public service administrators tend to demand a *high* level of assurance, so they are safe from accusations of risk-taking. However, although most Germans own a valid ID card, only about ten percent of them have ever digitally used the ID card. Services report dropout rates up to 80% as users are not able to navigate the ID card process.

Singapore

In 2022, there were 31,728 cases of reported scams which resulted in a total of SGD$660.7 million lost to scams[8]. Top five scam types of 2022 were phishing scams (7,097 reports), job scams (6,492 reports), e-commerce scams (4,762 reports), investment scams (3,108 reports) and fake friend call scams (2,106 reports). The breakdown of the total reported scams can be seen in Figure 3.

[6] eIDAS Levels of Assurance | europa.eu

[7] BSI - Federal Office for Information Security | bund.de

[8] Annual Scams and Cybercrime Brief 2022 |Singapore Police Force

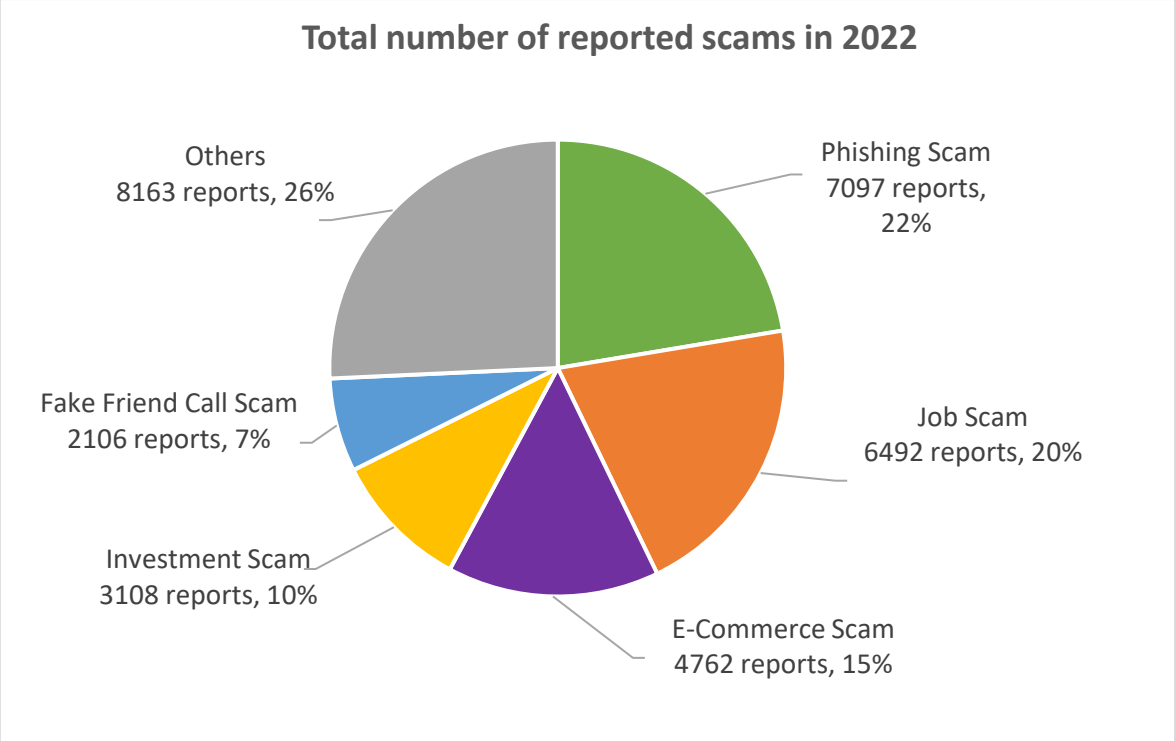

Figure 3: Total reported scams in 2022 (Singapore)

Among all scam types, phishing scams accounted for around 22% of total scams and was the highest reported scam type. The 7097 cases of phishing scams resulted in at least SGD$16.50 million of financial loss.

Generally, phishing scams involve the scammer tricking the victim into revealing their personal information such as login details. Once the scammer had obtained the victim's login details (ID and password), the scammer will access the digital services and perform unauthorised transactions.

The number of scams related to malware are of an increasing trend in 2023. Malware scam is currently the most sophisticated (both in terms of technology, and the technique used to convince users to install) and the most effective scam type observed.

New Zealand

In 2022, a total of 8160 incidents were reported to the Computer Emergency Response Team (CERT NZ)[9]. 22% of the incidents resulted in financial loss. The total loss amounted to NZD$20 million.

Among all incident types, phishing and credential harvesting is the highest reported incident type. This is followed by scams and fraud incidents that accounted for almost NZD$17.1 million of financial loss (86% of total financial loss). Breakdown of financial loss to the top reported scam types can be seen in Figure 4. Among all scam types, scams involving

[9] 2022 Report Summary | CERT NZ

unauthorised money transfer resulted in the highest financial loss, amounting to NZD$5.9 million (34% of total financial loss to scams).

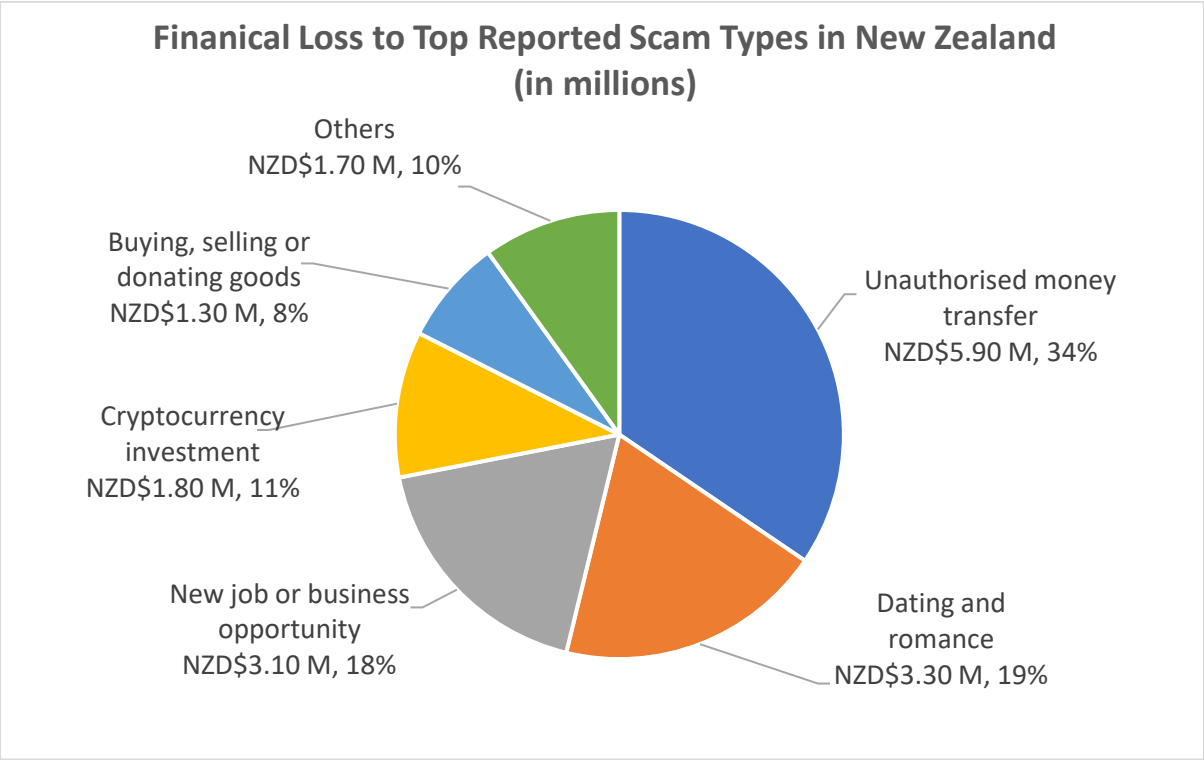

Figure 4: Financial loss to top reported scam types in 2022 (New Zealand)

As digital processes advance, scammers continuously adapt and target the weakest processes that reap the greatest financial gains. Poor initial entity binding done by authentic users gives way to impersonation and the creation of new accounts. Poor authenticators (e.g., login details) and authenticator binding allow scammers to impersonate victims and take over their accounts. Using the authenticator of the victim, the scammer can access services and make unauthorized transactions.

The DIWG findings elucidated the common scam types and modus operandi of scams across member nations. Scammers prey on victims via digital communication modes and seize control of victim's digital identity account and/or banking details to perform fraudulent transactions. With increasing digital advancements, scams are no longer bounded by physical borders. In fact, there are increasing cases of cross-border scams and digital identity misuse. The DIWG recognise the importance of discussing digital identity security on an international scale while acknowledging the localised differences. The following sections will expound on scam combatting measure across member nations and highlight collaboration opportunities for DIWG members.

4. Scam Combatting Measures

As digital security processes improve, cybercriminals pivot accordingly to the changes and launch more sophisticated attacks. Therefore, it is meaningful for the working group to collaborate and learn how to enhance the nation's scam defences and tactics from one another. A scan of working group members' scam combatting measures can be broadly categorised into five key domains:

4.1 Technology

Scams are becoming more prevalent and sophisticated with the rapid technological advancements. Scammers are now more technologically advanced and can exploit various technological advancement loopholes to trick their victims. The government has been and must keep up with the advancement of technology, continuously exploring and deploying new technologies to combat scams. Table 3 highlights the commonly adopted technological measures to combat cybercrimes of DIWG nations. Detailed case studies from DWIG members are expounded in this section as well.

Table 3: Technological measures to tackle scams

Track	Technological Measures
Fraud Detection e.g., Phishing Attempts	Tracking of anomalies through risk-based approach; Implementation of FIDO (Fast Identity Online) to deter phishing attempts
Challenge session during authentication	Step-up verification measures such as facial verification checks during authentication process (depending on the level of assurance required)
Case Management and Recovery	Case management to better track, manage and analyse cases.

1. Singpass – Singapore residents' digital identity has deployed facial biometrics as a form factor for high-risk transactions. The application also applied fraud analytics to detect anomalous transactions. Once anomalous transactions are detected, users would be required to do a step-up authentication, e.g., through facial scan where the selfie is matched against the photos held by the immigration authority. Other factors such as FIDO (Fast Identity Online) are being explored to tackle phishing. Additionally, in 2020, Singapore launched the ScamShield mobile app which identifies and filters out scam messages using AI technology. Since its launch, the ScamShield mobile app has blocked 200,000 scam calls and detected more than 3.5 million scam messages[10]. A new ScamShield Bot is also due for implementation via WhatsApp by 2023[11]. The

[10] Received a suspicious WhatsApp message? You can soon check if it's a scam | The Straits Times

[11] Anti-scam bot and monitoring service to detect spoofed govt websites among new digital tools| The Straits Times

ScamShield Bot works through police blacklisted contacts and links and crowdsourced reports. Users can check for scam signs by uploading screenshots or pasting suspicious links into the chatbot.

2. Since 2013, Israel had started issuing eID Identity Documents based on a smart card. The issuance was done by the Population and Immigration Agency which is also responsible for Border Control. The eID is based on international standards, such as the relevant parts of ISO/IEC 7816. It also has an authentication digital certificate for x.509 authentication based on challenge/response. A Digital Signature Certificate and digital signing is planned for future implementation. These certificates are issued by a Government CA operated by the Israel National Digital Agency.

   The eID card can be used to authenticate online with the Central Identity Management System and offline with special equipment like the self-service kiosks. The offline option embodies inclusivity and caters to individuals that do not have computers or card readers in their homes. Currently, Israel is piloting the usage of the biometric data that is stored on the eID to enable biometric face recognition and accessing digital services available on the kiosks.

   To combat scams, Israel adopts risk-based methods to detect and prevent malicious activities to the eID system. Online authentication information is logged to a separate environment which can be used to track anomalies and investigate specific suspicious cases. Additionally, Israel had developed a password recovery system. This password recovery system is an application that enables the release of PIN code or choice of new PIN code if the previous PIN code was forgotten. The application is now planning for nation-wide implementation.

   The actual usage of the eID card has been low due to the lack of card readers, people forgetting their passwords, and the availability of other means of online authentication which are based on mobile devices. To increase user adoption, the new generation of eID cards supports NFC. This implementation would allow mobile phones to be used as a reader to employ the eID card for authentication and digital signature. The new generation will dictate how the eID will prove its relevance as a form factor in the future.

4.2 Process (Collaborative and Rapid Information Sharing)

Scammers are becoming highly adaptable – they are prepared for their scam techniques to be exposed and have various ways to escape detection. It is thus important for governments to establish a clear and effective scam response process. The process generally involves dedicated teams that can rapidly respond to scam reports and disseminate information to key parties for real-time coordination. The scam response process is only effective through proper resource allocation, and more importantly, encouraging the private sector (i.e. banks) to take pre-emptive and preventive action to combat scams.

Private sector, especially financial institutions are targets of cybercrime relating to digital identity. Private sector entities should implement upstream measures to disrupt scams attempts. Banks, for example, can implement quick freezing of the customer's bank accounts if the account are compromised, or when suspicious activities were detected. Private sector should also share intel with the government on the trends and the type of scams that they are facing, to better facilitate investigation and improve the process taken to combat scams.

1. To better facilitate information sharing between the government and the private sector, Australia and Singapore have set up the Anti-Scam Centre, aiming to disrupt and prevent scams.

Table 4: Approach taken by Australia and Singapore for Process

Country	Approach
Australia	In May 2023, the Australian Government announced the allocation of $58 million to the ACCC to complete the set-up of the National Anti-Scam Centre (NASC) over the next two years. This includes a technology build of $44 million which will enable the NASC to receive a report of a scam from any institution (private or government) and centralise this intelligence; distribute data to those who need it most – such as banks to freeze an account, telcos to block a call, digital platforms to take down a website or account.
Singapore	The Anti-Scam Centre (ASC) of the Singapore Police Force was set up in 2019 to disrupt and prevent scam operations. This is done through quick response to scam reports and collaboration with banks to promptly freeze compromised bank accounts. Additionally, the Monetary Authority of Singapore (MAS) and Association of Banks in Singapore introduced an emergency self-service "kill-switch", allowing users to suspend their account quickly when their account is compromised. By working closely with the Monetary Authority of Singapore and local banks, the Singapore Police Force can freeze bank accounts suspected of being involved in scam activities within a day. This is a significant improvement from 14 to 60 days, which was the timeline for such operations in 2019. Between June 2019 and 2022, 40,900 bank accounts were frozen, leading to the recovery of more than SGD310 million, achieving a 25% recovery rate based on the reports[12].

2. In New Zealand, credit agencies are required to provide a person with a credit report that shows when and who has checked their credit history, allowing early intervention if financial fraud is intended. Individuals can place a 20-day hold on their credit history to prevent new financial accounts being created. For a fee, individuals can request to be notified if a credit history check is undertaken, forewarning them of potential fraud.

[12] Anti-Scam Centre of the Singapore Police Force: Fighting Scams is a Community Effort | Global Anti-Scam Alliance

4.3 Legislation, Policies & Regulations

Developing comprehensive and clear laws for digital identity protection and data privacy aids in safeguarding citizens' personal information. Additionally, legislation and regulations implemented can mitigate the risk of cybercrimes and protect citizens from scam attempts.

1. Australia and Singapore have similar regulations to safeguard SMS as a communication channel.

Table 5: Approach taken by Australia and Singapore for Legislation, Policies & Regulations

Country	Approach
Australia	In July 2022, the Australian Communications and Media Authority (ACMA) registered new rules to require telcos to identify, trace and block SMS scams. Under the rules, telcos must publish information to assist their customers in proactively managing and reporting SMS scams, share information about scam messages with other telcos, and report identified scams to authorities.
Singapore	The Infocom Media Development Authority (IMDA) launched the voluntary Singapore SMS Sender ID Registry (SSIR) scheme in August 2021. Post implementation, there was a 64% reduction in online scams via SMS in Singapore from Q4 2021 to Q2 2022. Following the success of the voluntary scheme, IMDA made it mandatory for organizations to register their SMS Sender ID under the Singapore SMS Sender ID Registry (SSIR) by 31 January 2023. All unregistered sender IDs sent to Singapore registered numbers will be blocked. Telecom operators have also implemented an SMS anti-scam filtering system as an upstream measure to prevent potential scam messages from reaching consumers. Key mobile operators have adopted machine-reading technology to identify and filter potential scam messages. Specifically, these solutions can detect malicious links within SMSes sent via telecom networks[13]. Additionally, IMDA and telco companies have been working closely in recent years to mitigate scam calls. Since 2019, commonly spoofed local numbers, (typically numbers impersonating local government agencies and emergency services) have been blocked. Since 2020, robocalls (automated scam calls) were blocked using pattern recognition technology. Overseas calls were also labelled with a "+" prefix to alert the public to be vigilant against unexpected international

[13] Proposals to strengthen safeguards for SMS messages to Singapore users: Implementation of anti-scam filter solution within mobile networks | IMDA

	calls. Currently, IMDA is exploring the option of allowing consumers to block international calls completely[14].

2. In July 2020, the New Zealand Cabinet agreed to establish the Digital Identity Trust Framework in legislation. This framework is a regulatory regime that will provide accreditation to compliant digital identity services and is the bedrock to establishing an accessible and effective digital identity system in New Zealand. The rules of the trust framework will provide minimum interoperability requirements, and a level of trust and security for both providers and people using tools and services within the system. Citizens can have greater autonomy over when and how they share their information online, have easier access to digital services, and benefit from reduced risk of identification and privacy breaches.

3. In Singapore, legislation was passed in May 2023 to target money mules that disclose their Singpass credentials or bank accounts to scammers[15]. The new legislation was passed to aid authorities in prosecuting offenders that assist scammers in money laundering. Under the new law, it is illegal for individuals to share their Singpass or bank accounts for criminal activities. Additionally, individuals can be deemed liable if they had received any gain for the disclosure and/or shared the credentials with someone they could not identify and locate.

4.4 Public Education & Awareness

Prevention is better than cure - public education and awareness empower citizens to practice good cyber hygiene, recognise common scam tactics and detect warning signs. As citizens become more vigilant against scams, they are less likely to fall for scam attempts. Additionally, when citizens are aware of the necessary scam reporting channels, they can participate in combatting scams through quick reporting and raising awareness among their family and friends. This will eventually create a ripple effect that spreads awareness and protect others from scams.

1. In Australia, the ACCC hosted Scams Awareness Week 2022 (7-11 November). With the support of over 350 partner organisations, the campaign encouraged people to learn ways to identify scams and to check whether an offer or contact is genuine before acting. The campaign had a potential audience reach of 82 million with 2,586 mentions in print, online, TV and radio.

   By the end of 2022, Scamwatch had 148,421 subscribers to its email alert service and published 13 media releases warning the public about scams. The Scamwatch website had over 6.36 million page views in 2022, and the ACCC's Little Black Book of Scams was viewed 49,247 times and downloaded 28,508 times. The Scamwatch Twitter

[14] Enhancing protection against scams IMDA proposes full SMS Sender ID registration as part the of ongoing measures | IMDA

[15] New laws passed to give police more powers to prosecute money mules, those who sell Singpass details to scammers | CNA

account (@Scamwatch_gov_au) posted 217 tweets and by the end of 2022 had over 37,000 followers. Additionally, the ACCC's Indigenous outreach team actively raised awareness about scams during visits to communities.

2. In Singapore, the Ministry of Home Affairs (MHA) launched a national anti-scam framework at the anti-scam seminar on 25 January 2023. A refreshed tagline - "I can ACT against Scams" was introduced during the seminar. The ACT acronym refers to the ACT framework of Add, Check, and Tell that members of the public can adopt to protect themselves against scams[16]. The public is encouraged to Add security features and download the ScamShield App, Check for scam signs, and Tell authorities, banks, and loved ones about scams. The ACT framework was introduced to bridge the awareness-action gap identified among Singaporeans. With this framework, the public can be more aware of cyber risks and adopt the necessary measures to safeguard themselves against scams.

   One way for the public to check on scam signs is via a trusted source like ScamAlert. ScamAlert is an initiative by the National Crime Prevention Council (NCPC) to educate the public on the recent scam types in Singapore[17]. When in doubt, members of the public are encouraged to check for scam signs via the site. The website contains the hotline for scam advice, common scam signs and types, sharing from scam victims, and various anti-scam educational materials. Individuals can chat with ScamAlert officers via the online chatbot and share their scam encounters with ScamAlert to warn others. Besides the website, the NCPC also provides WhatsApp and Telegram channels[18] to share scam alerts with members of the public who are subscribed. Subscription is free and the public is encouraged to share these alerts with their social networks to increase public awareness.

   The Singapore Police Force also continually alerts the public of the latest scam tactics via media releases and official advisories. One example would be the recent malware phishing cases targeted at Android users in Singapore. Advisories and media releases include scammers' modus operandi and reiterate precautionary measures such as the ACT framework that the public can adopt.

3. In New Zealand, there are various campaigns designed to increase public awareness: Privacy Week, Fraud Awareness Week, and Cyber Security Week. These campaigns include creating posters, social media posts and radio/tv broadcasts to educate citizens on best practices. The Department of Internal Affairs also runs Identification Management training course to educate relying parties and credential providers on how to implement better processes.

[16] How can you act against scams? MHA outlines 3 steps you can take | The Straits Times
[17] NCPC ScamAlert Website
[18] NCPC ScamAlert WhatsApp and Telegram Channels | NCPC Scam Alert

4.5 Recovery of Digital Identity

Similar to losing your personal identity card or passport, having your digital identity compromised or stolen causes great stress to our citizens. In cases where one genuinely falls prey to scams and has their accounts stolen, the time and process required for the citizens to retrieve their account should not be overlooked.

1. Australia's Scamwatch provided more than 116 disseminations of scam reports and intelligence on high risk or current scam trends to law enforcement, government, and key private partners. This intelligence assisted state and federal police to investigate and, in some instances, prosecute scammers. As a result of collaborative work by banks, law enforcement, and regulators, banks were able to distribute frozen scam account funds. The remediation enabled thousands of victims of the Hope Business scam to receive a portion of their financial losses back.

   Additionally, a non-profit identity victim support organisation - IDCARE was formed to address a critical support gap for individuals confronting identity concerns. They provide emotional support and advice on how to respond to identity theft.

2. In Singapore, the Singpass helpdesk and customer support have extended their operating hours from regular office hours to 24x7 to swiftly respond to scams.
   Members of the public can now contact Singpass operations immediately if they suspect that their accounts are compromised or to report suspicious activities detected. If call spikes beyond the helpdesk's capability occur, GovTech's national digital identity team members are also trained to be activated as helpdesk agents. These measures were taken as it was observed that attacks tend to happen at wee hours and on public holidays when victims may find it difficult to contact the helpdesk.

   Once a victim's digital identity account (Singpass) is reported as compromised, it will be immediately suspended. Upon completing the necessary investigations, the owner of the Singpass account will be able to reinstate their account by following the step-by-step account retrieval guide. If the account owner is not tech-savvy, they can visit the Singpass counters located island-wide to regain control of their accounts.

3. In New Zealand, scam victims and organisations affected by cybercrimes can seek assistance from IDCARE, a not-for-profit charity formed to address a critical support gap for individuals confronting identity and cyber security concerns[19]. To bridge the support gap, IDCARE connects the community to their expert Identity & Cyber Security Case Managers who listen and provide the best advice on how to respond to data breaches, scams, identity theft, and cyber security concerns.

[19] IDCARE

5. Collaboration opportunities with DGX Workgroup Members

As members of the DGX Digital Identity Workgroup, having active collaboration and knowledge sharing would be beneficial to our citizens, as we can react faster to the ever-changing threat landscape.

The findings from this report lay the foundation for future collaboration work among the members. Below are a few recommendations for members to consider.

With digitalization, scams are no longer limited by geographical boundaries. In fact, the DIWG has identified that transnational scams have been on the rise. As transnational scams occur beyond a nation's jurisdiction, it increases the difficulty of law enforcements to investigate and prosecute scammers. Thus, the DIWG hope to encourage international cooperation.

DIWG can have a quarterly exchange by sharing intel on the trends and modus operandi observed in their country. This can help the DIWG to better prepare for potential threats.

6. Annex [Detailed sharing from DIWG]

6.1 Australia

1. Trends

   Scamwatch is run by the Australian Competition and Consumer Commission (ACCC) Australia's national competition, consumer, fair trading, and product safety regulator. Scamwatch provides information to consumers and small businesses about how to recognise, avoid and report scams.

   - Scamwatch received **239,237** scam reports in 2022. This was a decrease of 16.5%.
   - 12% of people reported a financial loss and 27% reported the loss of personal information.
   - Total financial loss reported to Scamwatch was **$569 million** an increase of almost 76% on 2021.
   - The top 5 scam types reported in 2022 are:
     - Phishing scams – 74,573 reports
     - False billing scams – 27,488 reports
     - Online shopping scams – 17,886 reports
     - Identity theft – 16,212 reports
     - Remote access scams -11,792 reports
   - The top 5 scams by amount of financial loss were:
     - Investment scams - $377.2 million
     - Romance scams - $40.5 million
     - False billing scams – $24.8 million
     - Phishing - $24.6 million
     - Remote access scams - $21.7 million

2. Modus Operandi for digital identity observed:
   - In terms of contact methods (how the victim was contacted or came across scam):
     - Text message – 79,835 reports ($28.5 million lost)
     - Phone call – 63,821 reports ($141 million lost)
     - Email – 52,159 reports ($77.3 million lost)
     - Internet – 13,692 reports ($74.4 million lost)
     - Social media – 13,428 reports ($80.2 million lost)
     - Mobile apps – 10,058 reports ($71.6 million lost)

3. Countermeasure deployed and its effectiveness:
   - Disruption & law enforcement

- In 2022, the ACCC continued its work with other government agencies, law enforcement (in Australia and overseas) to share intelligence, disrupt scams and raise awareness in the community.
- Scamwatch provided more than 116 disseminations of scam reports and intelligence on high risk or current scam trends to law enforcement, government, and key private partners. This intelligence assisted state and federal police to investigate and, in some instances, prosecute scammers.
- Each week Scamwatch also sent lists of alleged scammer phone numbers to the telecommunications sector to inform their call and SMS blocking activities. Hundreds of millions of calls and SMS were blocked by telecommunications providers in 2022.
- The ACCC referred 1,757 web addresses to a third-party disruption service which were analysed during a 21-day trial. During this time, 381 were found to be malicious and 65 of those websites were removed preventing further harm to the community.
- As a result of collaborative work by banks; law enforcement and regulators, banks were able to distribute frozen scam account funds. The remediation enabled some of the thousands of victims of the Hope Business scam to receive a portion of their financial losses back.
- Scamwatch continued to share scam reports with the private sector. Reports where consent was provided were shared with the financial sector through the Australian Financial Crimes Exchange; Meta (Facebook); and Gumtree.

- Education & awareness:
    - The ACCC hosted Scams Awareness Week 2022 (7-11 November). With the support of over 350 partner organisations, the campaign encouraged people to learn ways to identify scams and to check whether an offer or contact is genuine before acting. Over 8 days, the Scams Awareness Week campaign had a potential audience reach of 82 million with 2,586 mentions in print, online, TV and radio.
    - By the end of 2022, Scamwatch had 148,421 subscribers to its email alert service and published 13 media releases warning the public about scams.
    - The Scamwatch website had over 6.36 million page views in 2022, and the ACCC's Little Black Book of Scams was viewed 49,247 times and downloaded 28,508 times.
    - In 2022 the Scamwatch Twitter account (@Scamwatch_gov_au) posted 217 tweets and by the end of 2022 had over 37,000 followers.

- The ACCC's Indigenous outreach team raised awareness about scams during visits to communities.
- Scamwatch staff presented at many forums in 2022 and conducted education activities and outreach.

- Policy, regulation, and advocacy:
    - In October 2022, the government announced seed funding for the ACCC to scope and plan a new National Anti-Scam Centre. In May 2023, the Government announced allocation of $58 million to the ACCC to complete the set up the National Anti-Scam Centre over the next two years. This includes a technology build of $44 million which will enable the NASC to receive a report of a scam from any institution (private or government) and centralise this intelligence; distribute data to those who need it most – such as banks to freeze an account, telcos to block a call, digital platforms to take down a website or account.
    - On 11 November 2022, the ACCC released the fifth interim report for the Digital Platforms Services inquiry. The ACCC has recommended a range of new measures to address harms from digital platforms to Australian consumers, small business, and competition.
        - The ACCC recommended targeted measures to protect consumer and business users of digital platforms against scams, harmful apps and fake reviews and
        - Minimum standards for digital platform dispute resolution processes and the ability for users to escalate complaints to an independent ombuds.
    - In July 2022, the Australian Communications and Media Authority (ACMA) - which regulates communications and media to contribute to maximising the economic and social benefits of communications infrastructure, services and content for Australia - registered new rules to require telcos to identify, trace and block SMS scams. Under the rules, telcos must also publish information to assist their customers to proactively manage and report SMS scams, share information about scam messages with other telcos and report identified scams to authorities.
    - In September and October, the ACCC participated in taskforces to protect consumers from the consequences of large cyber-attacks on organisations including those in the telecommunications and private healthcare sectors. These attacks exposed the personal information and identity credentials of millions of Australians. The ACCC produced information to assist the public to avoid the scams that followed the events and contributed to the development of a

scheme to provide access to information that could help prevent the misuse of the information.

- The government implemented data sharing arrangements pursuant to the Telecommunications Regulations 2021 to enable sharing of data between private sector entities who agreed to certain conditions outlined by the ACCC.
- The consequences of the cyber-attack included risk of identity misuse. The data breaches highlighted the significance of the earlier work by the ACCC, Department of Home affairs and other organisations to improve the ways documents are electronically verified (through Australia's Document Verification Service, DVS) and ability for people to obtain new credentials if they were at risk of misuse through the provision of unique identifiers on driver licences. As a result of card numbers being provided on licences and new fields becoming compulsory in the DVS in early September 2022, better protections were in place to protect consumers from identity misuse.

4. Collaboration opportunities with DGX workgroup members

    - Build awareness and share intel of contemporary security and scam trends to ensure members can build resilience into future planning.
    - Develop sharing models for successful and implementable strategies to combat online scams and strengthen protections for digital identities.

5. Use of e-ID card
    - N/A

6. Use of digital identity during times of emergency

    - One of the most common emergencies in Australia is bushfires. Australians with digital identities who lose their family's hard copy identification like birth certificates and passports, don't have to wait for replacement documents and can still access all the government services they need online.
    - A family affected by a natural disaster can save $128AUD in avoided costs and approximately 4 hours applying to replace identity documents and up to an additional 4 weeks waiting for the new identity documents to be created and sent.

7. Further comments
    - Australia's 2022 data is included in the Targeting Scams Report https://www.accc.gov.au/about-us/publications/serial-publications/targeting-scams-report-on-scams-activity
    - The Report includes data from a range of Australian organisations including the Australian Cyber Security Centre's 'reportCyber'; Australian Securities and

Investments Commission; the Australian Tax Office; banks which provide data to the Australian Financial Crimes Exchange; IDCARE (an identity victim support organisation) and other participating government organisations.

6.2 Germany

1. Trends/ regulatory setting
    - Phishing and scamming is one of the most relevant hurdles when talking about secure digital identities.
    - Digital identities are a widely discussed topic across the European Union, where the goal is to standardize the access for citizens across the EU while standardizing the technical security standards at the same time.
    - The European Union's sets the common frame for digital identities in the EU. It includes level of assurances, which distinguish digital identities according to their level of security:
        - *Low*: for instance, a username and password are used for self-registration on a webpage;
        - *Substantial*: for instance, a username and password are followed by a one-time password sent to your mobile phone;
        - *High*: for instance, enrolment is performed by digitally reading out a national ID Card.
    - There is now a second version of this law in discussion, eIDAS 2.0, with the goal to set the regulatory framework for an EU-wide ID-wallet. Security issues are being considered by all European security agencies, who form an expert group which informs the law-making process. Germany is represented by the Federal Office for Information Security.

2. Modus Operandi for digital identity scams observed:
    - Looking at which levels of assurance are applied by services directly correlates with the possibilities for fraud. Whereas *low* levels of assurance in digital identities represent the most widespread solution for end users, they also incorporate the greatest risk for phishing or similar attacks. Digital identity cards on the other hand, which ensure a *high* level of assurance, only have a low market reach although their security level has proven to be almost impeccable.
    - Among other European countries, France launched a widely successful digital identity called France Connect. It mainly addressed the *low* to lower *substantial* security level. They report that fraud is so widespread that they now are looking to additionally offer an identity service with a strong *substantial* level.
    - Germany has one of the most restrictive understandings regarding data and information security. Especially in the public sector, citizens are usually required to identify on a *substantial* if not *high* level for any service they want to use. Public service administrators tend to demand a *high* level of assurance so they are safe from accusations of risk taking. The downside is, although most Germans own a valid ID card, only about ten percent of them have ever digitally used the ID card. Services report dropout rates up to 80% as users are not able to navigate the ID card process.

3. Countermeasure deployed and its effectiveness:

- The level of assurance is being increased for critical processes in services. This can be observed in the private sector as well as the public sector.
- In the private sector, *substantial* two-factor authentications become widely applied e.g. for banking account transactions (via TAN generating apps), or when setting back passwords for accounts.
- In the public sector, France introduced France Connect+ with an increased security level and is considering introducing an identity card for the *high* level.
- In Germany, the usage of the *high* level identity card requires multiple prerequisites, which many don't fulfill and hence keeps them from using it:
    - German-, EU- or residence-permit- **ID card**
    - A **personal PIN** has to be set once after receiving a one-time PIN via letter when a new identity card is issued.
    - People who forget their personal PIN have to apply for a new letter.
    - An **app** is required, which reads out the card's data. The identity cards incorporate an NFC chip, which can be read out via a card reader or all smartphone models with a NFC function.
    - **Scanning** the ID card takes some practice. The antenna in smartphones is not that strong (not comparable to NFC card readers), hence a user has to find out how to best hold the card to the smartphone, as well as hold it there for about five seconds.
- The way this German ID-system is set up is extremely secure and has not been hacked. There is the app "AusweisApp2", which has been available for more than six years, but did not reach a wide user base. We are currently working on increasing the digital usage of the ID cards via an improved app, "BundesIdent", which especially iterates the service design for first time users. People who used the ID card once to identity themselves online for a service and don't forget their PIN, find it easy to use on different occasions.
- The private sector on the other hand rarely requires the usage of a *high* level via the identity card and also has alternatives which are more accessible, without requiring a PIN, and more widely known among users. For instance, new bank accounts can only be opened, if the new user is identified carefully. For German banks, identification is allowed via an agent-video-call, hence the identity card is usually not used there.
- This combination of stagnating low user acceptance of using ID cards online and low offer of use cases kept the adoption of the ID card at an underwhelming level until now.

4. Collaboration opportunities with DGX workgroup members
    - To use the ID card with the AusweisApp2, requires users who identify on a desktop to download and link a desktop app to the corresponding smartphone app. This process is highly unusual for user behavior and is hence rarely used.
    - With the new BundesIdent app we are currently looking into a phishing-proof way to do identification while switching devices (desktop/ mobile), based on the WebAuthn standard. Any input or experience is welcome. The goal is to maintain

the high standard of the desktop app solution, while offering a more user friendly approach.

6.3 Israel

1. Trends
    - We do not have statistical data at this stage. Hopefully, we will have some data we could share in the future. We are going to start a new study on these issues.
2. Modus Operandi for digital identity scams observed:
    - We do not have data at this stage. Hopefully, we will have some data we could share in the future. We are going to start a new study on these issues.
3. Countermeasure deployed and its effectiveness:
    - We use different methods and techniques already as risk-based methods to detect and prevent malicious activities to the system.
    - Online authentication information is logged to a separate environment which can be used to track anomalies and also investigate specific suspicious cases.
4. Collaboration opportunities with DGX workgroup members
    - The group holds opportunities to engage and learn from other participants experience in the digital identity field. Specifically, we are currently analysing an organizational scheme to deal with the issue discussed. When we will organize the basic concept, we will be able to discuss it further with the workgroup members.
    - Also, we have raised the notion of a possible international collaboration regarding digital identity misuse, as these happen on an international basis. Therefore, much could achieved by setting up international framework for that end, discuss such issued deeper and later on even share specific warnings, risks and operational cooperation.

5. Use of e-ID card
    - Israel started issuing eID Identity Documents based of a smart card, since June 30th 2013. The issuance is done by the Ministry of Interior agency, called the Population and Immigration Agency which is also responsible for Border Control.
    - The eID is based on international standards, such as the relevant parts of ISO/IEC 7816. The eID has an authentication digital certificate for x.509 authentication based on challenge/response.
    - A Digital Signature Certificate and digital signing is also planned for the future.
    - The certificated are issued by a Government CA operated by the Israel National Digital Agency.
    - The eID card is used both to authenticate online with the Central Identity Management System, and with special equipment like the self-service kiosks that are used to enable digital services that do not have computers or card readers at their homes.

- We are now piloting the usage of the biometric data that is stored on the eID to enable biometric face recognition, and thus accessing digital services available on the kiosks.
- One application is actually enabling releasing the PIN code or choosing a new PIN code if the previous one was forgotten. We are now in a phase of discussing the implementation on a nation-wide scale.
- The actual usage of the eID card has been low due to a few reasons: The lack of card readers, people forgetting their passwords, and the availability of other means of online authentication which are based on mobile devices.
- The new generation of eID cards supports NFC, so the idea is that a mobile phone would be used as a reader to employ the EID card for authentication and digital signature.
- This new generation will dictate how the EID will prove its relevance as a form factor in the future.

6. Use of digital identity during times of emergency
    - Digital Identity becomes an important tool enabling digital services during times of emergency. Such were the times of the pandemic, but the same is true to similar incidents, like – earthquakes, other natural disasters, or a state of war or situations when people have limited mobility possibilities.
    - The Central National Identification System had a boost in the numbers of online registration during the pandemic, which enabled the state to deliver digital services in an efficient way.
    - Further development in distributes tools such as the mobile wallet, will probably strengthen this capability.

7. Further comments
    - The fact that this group focuses on the issues of integrity, fraud and the ways to combat them, is important as it highlight of this issue which becomes more important as more critical and privacy related services are put into action, thus calling for continuous activity to protect the integrity of the digital identity.

6.4 Singapore

1. Trends
    - The number of scam and cybercrime cases increased by 25.2% to 33,669 in 2022, compared to 26,886 cases in 2021.
    - The top 5 online scam types recorded in 2022 are:
        - Phishing scam (22.4%)
        - Job scam (20.5%)
        - E-commerce scam (15%)
        - Investment scam (9.8%)
        - Fake friend call scam (6.6%)

2. Modus Operandi for digital identity observed:
    - The scammer will first obtain the victims login details (ID and password), and takeover the account of the victim.
    - Using the identity of the victim, the scammer will then access the digital services, and make unauthorised transactions.

3. Countermeasure deployed and its effectiveness:
    - Cross agencies effort
        - ScamShield mobile app jointly developed by National Crime Prevention Council (NCPC) and GovTech identifies and filters out scam messages using AI.
        - IMDA made it mandatory for organizations to register their SMS Sender ID under the Singapore SMS Sender ID Registry (SSIR). All unregistered sender IDs will be blocked. Additionally, telecom operators have implemented SMS anti-scam filtering system that can prevent potential scam messages from reaching consumers.
        - Monetary Authority of Singapore and Association of Banks in Singapore introduced an emergency self-service “kill-switch”, allowing users to suspend their account quickly when their accounts are compromised.
    - Public Education
        - Ministry of Home Affairs, Singapore Police Force, and NCPC organised campaigns to educate and encourage members of the public to translate scam awareness into action by proactively adopting anti-scam measures.
        - Posters on public transport, social media posts and radio broadcast to educate citizens on best practices while transacting online.
    - Strengthen Singpass
        - Having a strong authentication factor would lower the success rate of scammers taking over user’s account. We have introduced facial

biometrics as a form factor for high-risk transactions and are exploring other form factors as well.
- Applied Fraud Analytics to detect and block anomalous transactions.

4. Collaboration opportunities with DGX workgroup members
    - Mind share on latest security and scam trends.
    - Share measures implemented, and exchange intel on combatting online scams and its effectiveness.

5. Use of e-ID card
    - During our initial phase, studies showed that it is challenging for users to have a digital identity in the form of a smart card or hard token as users would need to carry an additional card / token. In addition, users would need a card reader to make transactions. There are overheads for issuance and distribution as well, which may not be cost effective and scalable.
    - Users of Singpass are onboarded via a national registry and issued with a digital certificate on the Singpass app.
    - Currently, 97% of Singapore Citizens and Permanent Residents are onboarded to Singpass. With a high rate of mobile phone usage of 153.8% of smartphone penetration in Singapore, about 90% of the total Singpass transactions are performed via the Singpass app.

6. Use of digital identity during times of emergency
    - During the COVID-19 pandemic, we pivoted Singpass to support the national check-in system (SafeEntry), that logs individuals visiting public venues such as malls and workplaces, allowing quicker contact tracing. This has shown that with a foundation digital identity, they can be pivoted to support times of emergency.

6.5 New Zealand

1. Trends
    - The number of incidents reported to the Computer Emergency Response Team (CERT NZ) decreased by 8% to 8160 in 2022, compared to 8831 incidents in 2021[20].
    - The top 5 online scam types recorded in 2022 are:
        - Unauthorised money transfer (NZ$5.9m)
        - Dating and romance (NZ$3.3m)
        - New job or business opportunity (NZ$3.1m)
        - Cryptocurrency investment (NZ$1.8m)
        - Buying, selling or donating goods (NZ$1.7m)

2. Modus Operandi for digital identity observed (identity theft):
    - Scammers target the weakest processes with the greatest gain. Shift focus and channel as processes improve.
    - The development of better ways to *verify information is true* has resulted in an increase in information theft risk and more attacks on poor processes for checking that *the information belonged to the claimant*. This has been compounded in the digital channel by limited digital options equivalent to manual entity binding processes (until recently).
    - Scammers utilise the over-collection of information to obtain source information for impersonation. Poor initial entity binding allows impersonation for the creation of new accounts.
    - Poor authenticators (e.g. login details) and authenticator binding allow for control of the victim's account.
    - Using the authenticator of the victim, the scammer can access services, and make unauthorized transactions.

3. Countermeasure deployed and its effectiveness:
    - Credit agencies and Credit reporting
        - Credit agencies are required to provide a person with a credit report that shows when and who has checked their credit history, allowing early intervention if financial fraud is intended.
        - People can also place a 20 day hold on their credit history to prevent new financial accounts being created.
        - For a fee, people can also request to be notified if a credit history check is undertaken, forewarning them of a potential fraud.
    - Public Education
        - There are various campaigns designed to increase awareness throughout the year, for example, Privacy Week, Fraud Awareness Week and Cyber Security Week. These include creating posters,

[20] https://www.cert.govt.nz/about/quarterly-report/2022-report-summary/

social media posts and radio/tv broadcast to educate citizens on best practices.
    - Agencies such as CERT NZ and Netsafe provide online resources to help people learn about self-protection.
    - The Department of Internal Affairs run Identification Management training course to educate relying parties and credential providers on how to implement better processes.
- Standards, services and frameworks
    - There are a number or recommended standards that, if complied with, would have an impact on the incidence of identity theft.
    - The Digital Identity Services Trust Framework is a regulatory regime that will provide accreditation to compliant digital identity services.

4. Collaboration opportunities with DGX workgroup members
    - Share latest scams and trends.
    - Share measures implemented, and
    - Exchange intel on combatting incidents and their effectiveness.

5. Use of e-ID card
    - New Zealand does not have a National ID.
    - RealMe® is a government run opt-in authentication and information assertion service for both citizens and relying parties. The challenge has been to align uptake with the services that could consume it. It currently provides only a limited number of attributes, and has not met the needs of users or relying parties when it comes to improving enrollment efficiency.
    - There are currently 1,178,288 RealMe verified identities.

6. Use of digital identity during times of emergency
    - RealMe verified identity was an onboarding option for the NZ Covid Vaccine Pass during its roll out. This was an alternative option to the Ministry of Health enrolling users with their own verification processes.