JOINT COMMITTEE ON LAW ENFORCEMENT

THE CAPABILITY OF LAW ENFORCEMENT TO RESPOND TO CYBERCRIME

SUBMISSION II

QUEENSLAND WHISTLEBLOWERS

Whistleblowers Action Group (Qld) Inc

27 AUGUST 2025

CYBERCRIME AND RISK MITIGATION

Submission by
Whistleblowers Action Group (QLD) Inc
27 August 2025

Overview

QWAG has taken advantage of the two parts to this Senate Inquiry to build a Risk Management Analysis for the prevention of cybercrime, based on the wealth of relevant statistics and authoritative opinions provided by submissions made to the first part of this Inquiry.

Based on this Risk Analysis, we have reached a view that building a system for Online Financial Transactions {hence OFTs] that does not include the continuance of Off-line options [hence OFFOs] may bring and then establish the most serious financial vulnerabilities to the economy, its major entities, and to its lower level participants. In particular:

- The threat already posed to our economy and financial system from enemy states and international criminal organisations will be greatly magnified from the situation now where OFFOs would support an immediate alternative to OFTs in trouble; and
- OFFOs would continue to provide a simple, understandable alternative to those many Australians who have been disabled, naturally or by loss, from reasonably safe operation of their income and or wealth using OFTs.

QWAG makes the analogy with the use of stairwells and elevators in high-rise buildings. The switch to the use of elevators for moving between floors and the entry / exit portals was sensible and quickly taken up, as the switch benefitted all – the switch grew the economy which had then the ability to reach greater heights in buildings and skyscrapers. But our jurisdictions do not allow the construction of multi-story buildings and skyscrapers without the continuing inclusion of stairwells or multiple stairwells. This is because, as well as the acknowledged benefits from elevators, there are also catastrophic risks with elevators. Any fire alarm coming from any room on any story of a multi-story building will deny the use of elevators by those seeking safety from any spread of the fire. Those survivors from above the impact level in the enemy attack upon the World Trade Centre on '9/11' used the stairwells, as did those from below the impact area – that is the route that the firefighters also took in their efforts to rescue people.

Purpose

We thus seek to influence the second part of this Inquiry to

- Consider and build upon the Risk Analysis that we offer herein;
- To consider the risks and their mitigation where Australia's financial system depends on the safe operation of OFTs only;

- To consider the risk mitigation that may be available if selected OFFOs are maintained (in addition to the limited uses of cash already foreseen by the government). We make reference herein to the bank cheque posted to Post Office Boxes at an authorized Australian Post Office for effecting large transfers (as may be used by a retiree moving investment funds to a term deposit at another bank or another investment vehicle in order to secure a higher interest rate; or for contractor payments or law case settlements, etc;
- To consider the protection of users of any continuing OFFOs from mistreatment by entities seeking to force OFTs upon them; and
- To consider the publication of statistics upon the use of particular OFFOs whose operation may have been misrepresented by those pursuing OFTs ONLY operations for their business or their administration or their services.

Risk Analysis

In **Appendix A**, we have assembled all the information , including relevant statistics and authoritative opinions, on cybercrime from submissions made during the first part of this enquiry. We have done this organized under the typical headings used to report upon a Risk Analysis. Where relevant and / or available, we have added a comment about the relative risk from the use of one form of OFFOs, the bank cheque passed to Post Office Boxes (not front yard fence letterboxes, based on our own studies.

The Headings used are as follows:

Consequence / Impact / Damage – 16 extracts from submissions made to Part 1 of this Inquiry.
Likelihood – 6 extracts.
Exposure – 27 extracts.
Liability – 6 extracts.
Attraction – 28 extracts.

The risk is not just the immediate use of the bank details to achieve theft or fraud, but how the information can be used in scams that rely on perceptions of validity conveyed to the bankee or payer by the use of true and recognizable bank data and copied business letterheads, logos and layouts.

A few selected summary quotes may summarise the risks that need mitigation in Australia's situation:

"… customers continue to bear losses that they have limited ability to prevent" [ACCC].

<u>The most educated are the most susceptible</u> – ***"Respondents who used various online safety measures had a higher prevalence of cybercrime victimization"*** [AIC]**. *"… only 9.6% of participants demonstrated sufficient skills and knowledge to detect and prevent scam attempts*** [IDCARE]

<u>Cybercrime is</u> ***"a challenge that resists solutions"*** [IDCARE]

> ***"These capability gaps are amplified by increasingly complex and technologically sophisticated offenders and offences, which also undermine police surveillance and evidence-gathering efforts"*** [AIC]
>
> ***"One report to Report Cyber every 6 mins – far outweighs the capacity of law*** **enforcement"** [AIC]
>
> ***"… Australians are acutely aware of the very real risks of cybercrime and are seeking more control over the collection and use of their personal information"*** [OAIC]
>
> Australians are growing a ***"… loss of confidence in the internet "*** [AIC]

These factors reflect the role played by the human factor and how the human factor ***"extends to the notion of 'usable security' - …designed to be user-centric, inclusive and affordable"*** [CCRT-DU].

The online system has not been designed for the protection of customers. The system has failed by design in this vital respect.

The failure of online systems caused by the **Microsoft / Crowdstrike *'unforgivable'*** mistake, when under friendly fire rather than under fire from a criminal state – affecting banks, health services, ship docks, media companies, casinos, airports, water authorities, retailers and airports – demonstrates the inherent widescale vulnerability of the workings of online system to the smallest error or act of negligence.

For customers forced to use online systems, the smallest error by the customer or by the bank or by the trader can lead to the customer losing all of their funds, with little if any chance of the funds being recovered from the fraudster, and with every chance of the trader and the bank being able to deny liability under law and refuse compensation or reimbursement.

RELATIVE RISKS ASSOCIATED WITH ON-LINE v OFF-LINE FINANCIAL TRANSACTIONS

History. The comparison of on-line versus off-line financial transaction systems may have been characterized to date by mere assertions. The assertions made to the public have been made by entities with a financial plan based upon the termination of off-line systems and the universal adoption of on-line systems for financial transactions. Mere assertions are not a valid basis for any risk management plan by investors for maximizing their funds.

The assertions at issue for the last two decades may be represented by the claim that on-line systems are safer and faster, and have become the choice of 90% of consumers. In most explanations of the reasoning behind these assertions, the **"safer"** claim tends to be based on the vulnerabilities of a cheque being delivered to a letterbox on a front yard fence, that may be easily accessed. The **"faster"** claim appears to be based upon the speed of electrons compared to the suburban street 'Postie'. The

"choice" claim may usually be attributed to the droppage in postal volumes over the last two decades and the resultant increase in the cost of stamps.

The Re-consideration. These assertions and the common perceptions used to project credibility to these assertions may have come under re-examination because of the question now being put to financial authorities and entities - whether or not the on-line financial transaction system is or is not fit for purpose, or is or is not in a state of irrecoverable failure.

Statistics provided in 2024 by financial experts and responsible entities are offered in Appendix A to justify why the question of **fit-for-purpose** is being posed, if not to expose the perception that many failures of the on-line system may have been silently accepted.

Advocates of the on-line financial transaction system are no longer claiming that the on-line system is **"safer"**. Similarly, the speed of the electron in now regarded as a threat to the safety of any financial transfer, through the assistance it gives to the operations of scammers and hackers in their immediate escape. In response to this threat, financial entities may be choosing to slow down their off-line internal financial processes, including approvals and clearances, in order to give the on-line systems and their operators time to identify any hack or scam, and time to uncover any scam – such slowdowns thereby are enabling a better chance of recovering what the speedy electrons have attempted to steal.

The re-considerations are also providing consumers an opportunity to assemble information on the tactics that were used to coerce or to cajole consumers into withdrawing from the use of cash, of personal cheques, of bank cheques and of other forms of off-line financial transfer processes. Forms of treatment that may constitute coercion may include:

1. Delaying processing of cheque payments received until after renewal dates or payment deadlines, such that consumers suffer late payment fees (e.g. payments to telco's), or lose protections (e.g. insurance cover), or lose membership (e.g. to professional associations) – customers have been forced to adopt the specific on-line processes of the entity in order to preserve their service-cum-protections-cum-memberships, and/or maintain their current cost of living;

2. Refusing payments of moneys held belonging to consumers / investors except by on-line means, denying interest being paid for moneys withheld for several years, sending moneys that have been claimed by investors (say, in writing and /or with stamped, self-addressed envelopes, and / or with reasonable payment for any extra cost of using an off-line process) to government unclaimed money offices, falsely informing authorities (e.g. Australian Taxation Office) that the moneys have been passed to the owner when the funds have been withheld.

Both examples may have similarities with the cybercrime, **'ransomeware'**, where the scammer threatens adverse consequences if funds are not handed over to the scammer's crypto bank account.

An Off-line Alternative. A bias in the advocacy for on-line financial transactions may have been portrayals of the off-line alternative as occurring only in loose situations that typically occur for the postal delivery of cheques to a letterbox on a front yard fence, or to a converted-milk-container mail box beside the roadway entrance to a rural property. The off-line alternative posing real competition to the on-line systems for many (not all) recipients of funds may be the PO Box in the wall of a registered Post Office, instead of the letterbox on a suburban front yard fence. The PO Box has the protection of the security systems used at registered Australian Post Offices (locks, lighting, public in attendance, cameras, etc).

The problem, however, for advancing the relative merits of the PO Box is that relevant data on losses from bank cheques stolen from PO Boxes does not appear to be available.

There are figures on proxies for Break-ins-to-PO-Boxes. These include:

1. Prosecutions for forgeries using cheques;
2. Apprehended persons for postal offences; and
3. Number of postal offences.

So, figures from the Queensland Police have been reported for a five year period ending in 2021, where **fraud by cheque** carried out in all ways (not just by stealing from locked PO Boxes at post office buildings and through the security systems at those buildings) was **reduced by 43% to 16 incidents in 2021**. The Australian Federal Police replied to our inquiries for the ACT, where there were 2 cases of postal offences (from 1 person) in 2023. Our requests for statistics from the Australian Bureau of Statistics [ABS] were refused on the basis that ABS does not hold the data, the ANZSOC codes for the data described on the ABS website being outside the scope of the Recorded Crime collections, ABS advised. Requests for such data made to postal authorities did not attract an acknowledgement of the receipt of our data request, or a reply.

It appears that there may be so few instances of break-ins to PO Boxes at registered Post Offices (fewer cases where cheques are stolen, even fewer where fraud is attempted using cheques stolen from PO Boxes), that authorities are not collecting direct data on the performance of the PO Box as a protective device and service for safe transfer or funds by cheque.

A Security Plan for Individuals and Families

At Appendix B we have outlined the current factors that may guide an individual or family to the development of their own cybersecurity plan that may steer them to different choices of OFTs and / or OPPOs for different purposes in different circumstances.

Summary

An impressive building of the facts, statistics, factors, and expert opinions into summary conclusions about the on-line financial transactions system in Australia has been provided by Law & Cyber. Their submission to the Senate Inquiry into Cybercrime stated that the banking sector has failed to adequately protect consumers from fraud during the change from cheque-based payments to electronic banking, and argues that financial services like banking should be fit for purpose. The observations by this expert in practice, in all areas contributing to the failure, namely:

Legislation –

- banks are allowed to transfers funds to cryptocurrency;
- banks are not required to do name checks;
- technology firms are allowed to set liability caps to minimal levels even in the case of negligence or breach of contract; and
- millions of organisations are allowed to forcibly and / or coercively collect databases of personal information.

Technology –

- technology is enabling fraud more than it is preventing fraud;
- technology is facilitating the deception that underpins vulnerability; and
- technology companies use the option to 'blame people' when people suffer losses, and not blame the ease with which cybercriminals can utilize the banking system to defraud Australians.

These few of the many factors contributing to the failure of the system may be a complete demonstration that the on-line financial transactions system in Australia is not fit for purpose.

The online system, the assemblage of information is tending to show, may not have been designed for the protection of customers. The system appears to be failing by design.

We repeat the point that the failure of on-line systems caused by the **Microsoft/Crowdstrike *'unforgivable'*** mistake, when under friendly fire rather than under fire from a criminal state – affecting banks, health services, ship docks, media companies, casinos, airports, water authorities, retailers and airports – demonstrates the inherent widescale vulnerability of the workings of the on-line system and its OFTs to the smallest error or act of negligence.

For customers forced to use online systems, the smallest error by the customer or by the bank or by the trader can lead to the customer losing all of their funds, with little if any chance of the funds being recovered from the fraudster, and with every chance of the trader and the bank being able to deny liability under law and refuse compensation or reimbursement.

G. M. McMAHON
Secretary,
QWAG

APPENDIX A TO
CYBERCRIME AND RISK MITIGATION
DATED AUGUST 2024

STATISTICS ON THE PERFORMANCE OF THE ON-LINE FINANCIAL TRANSACTION SYSTEM

Submissions to the Senate Inquiry set out the effects and consequences of fraud and scam operations undermining the on-line system for financial transactions. Below are set out these statistics under headings that may be used by an organized risk analysis.

Consequence/Impact/Damage – It may be argued that an intercepted cheque puts a limited amount at risk. Giving details of a bank account that is on-line, however, puts all funds in the bank account at risk.

The **Australian Signals Directorate** [hence 'ASD'] reports that in 2022-23, ASD responded to 127 extortion related incident, with 118 of these incidents involving ransomware or other forms of restrictions to systems. ASD also responded to 79 cyber security incidents involving hacktivists' denial-of-service (DoS), more than double the previous year, and the self-reported cost of cybercrime to business through ReportCyber was $80 million, a 14% increase.

South Australian Police [hence 'SAPOL'] ***"utilises the ReportCyber platform …, but there are limitations in the size of data sets that can be shared across this platform".*** And this is the ***"database of victim reported cybercrime and a repository for information relating to suspicious social media accounts and fraudulent bank accounts".***

There were 143 cyber security incidents related to critical infrastructure [ASD]

The tax commissioner [hence 'ATO'] stated that ***… the risk of sophisticated fraud attempts through the increase in enormous data theft will only continue to grow.***

One report of a cybercrime against Australians is being made to ReportCyber every 6 minutes [Submission 3 by Australian Institute of Criminology, hence 'AIC']

Domestically, cybercrime cost $33billion in 2020-21 [Submission 4 by Cyber Security Cooperative Research Centre – hence 'CSCRC']. Total estimated economic impact on individual Australian computer users has exceeded $3billion [AIC]

Two thirds of Australians aged 15 years and over were exposed to a scam in 2021-22, according to the Australian Bureau of Statistics [hence 'ABS'].

In more than 13,000 cases the frauds were committed using bank transfers which remains the most reported payment method for scam losses (Law & Cyber, hence 'LaC')

72,000 reports from Australians aged over 65 (were made) ***last year … Financial regulator ASIC took down 4200 investment scam websites last year*** (Australian Treasury)

Each small business is losing each year an average of $46,000 – medium business is losing $97,200 on average [Submission 15 by the Australian Banking Association – hence 'ABA']

An estimated $4billion was lost to scams in 2022 [Submission 12 by the Attorney General's Department – hence 'AGD']

Cybercrime impacting the Australian Community is significantly increasing:

> ***"The frequency of cybercrime is also increasing. In 2022-23 there were 94000 cybercrime reports (1 every 6 minutes) which was a 23% increase on the previous year. … The average cost of cyber incidents to Australian businesses and individuals has also increased"*** [AGD]

In 2023 Australians reported to Scamwatch $158.3 million losses where cryptocurrency was the payment method. This represents a 12% increase compared to the same period in 2022. [Submission 17: Australian Competition & Consumer Commission – hence 'ACCC']

In NSW, there was a 42% increase in all cybercrimes during the 3yrs to June22. Cyber fraud increased by 95%. Queensland and Victoria recorded disproportionately higher rates of cybercrime relative to populations [CSCRC]

The compromise of Medibank Private led to the unauthorized release of 9.7 million records of personal information [ASD].

There has been a threefold increase in data breaches during 2021 to 2023. [AIC].

Likelihood – It may be argued that criminal rogue states are chasing account information by internet whereas no reported attempts are in evidence of attempted break-ins by rogue states into locked post office boxes at authorized Australian Post Offices.

The AGD recalled the major data breaches that had occurred at Medibank, Latitude, Optus, and HWL Ebsworth. These and other such data breaches ***'significantly increase the likelihood of online scams and fraud'*** [AIC]

Two thirds of users (67%) have already become a victim of at least one type of cybercrime during their lifetime [AIC], and 43.1% of all victims have experienced multiple types of cybercrime [CSCRC]

In the 12 months prior to survey, 47% of users experienced a cyber loss [AIC]

Regarding fraud, computer misuse accounts for nearly half of all self-reported crime incidents [AIC]. Eight percent (8%) of respondents were victims of fraud and scams in which they paid money or provided sensitive information. Seven percent (7%) of scam and fraud victims lost more than $10,000, and 1.7% of these lost $100,000 or more [AIC]. On-line fraud and scam victims lost more money than the victims of other cybercrimes, and experienced more negative outcomes, especially practical, social and financial harms [AIC]

The ATO says the sophistication of new attacks is making it harder for people to spot a fake.

Exposure – It may be argued that a cheque is in transit inside the post office security and controls for a day or a few days, while a firm and a government department hold bank account data for years (a greater time exposure).

Only 23% of organisations ***'reported having effective processes to manage info security risk'***, and only 12 % of respondents agreed they were regularly conducting cybersecurity awareness training [Submission Sub 6: Australian Charities and Not-for-Profits Commission – hence 'ACNC'].

"$33billion … lost as a result of cybercrime in 2020-21 … is only expected to increase" [AGD]

Law and law enforcement cannot keep up with the exponential changes in technology [LaC]

Organisations collect vast amounts of data about Australians and continue to obtain significant financial benefits from technology while passing on what can be serious risks to consumers, who do not appreciate the significance of those risks [LaC]

"In the last 12 months alone, IDCARE demand from the community has increased over 20%, recording over 81,000 individual cases, that resulted in over 260,000 engagements. The vast majority of these community contacts result from crimes enabled via the online environment, resulting in nearly half a billion dollars in lost value [Submission 10: Identity Care Australia and New Zealand -hence 'IDCARE'].

"… we can realistically expect the volume and complexity of cybercrime will only accelerate" [Submission 7: Centre for Cyber Resilience & Trust, Deakin University -hence 'CCRT-DU']

… millions of Australians (are) ***having their information stolen and leaked on the darkweb*** [ASD]

51% of common passwords can be cracked instantly, 81% of all passwords can be cracked in a month [LaC]

The Northern Territory Police have admitted that ***"current NT legislation is not fit for purpose in the digital age".***

Cybercrime continues to evolve as a result of advances in communications technology, increased connectivity and increased engagement online [AGD]

Advancements in AI, deep fakes, and related technologies, combined with ongoing challenges with encryption, cryptocurrency detection and identity obfuscation is likely to mean that cybercrimes will continue to grow along with their sophistication [IDCARE].

There is a … decline in the quantity and quality of cyber security reporting to the ASD [ASD]

Technology is a twin edged sword when it comes to finding solutions to cybercrime. IDCARE put it succinctly.

- Cybercrime is ***"a challenge that resists solutions"*** ;
- A problem that ***"cannot be solved in a single domain"*** ; and
- ***"…a critical part of any solution (technology) is perversely also an enabler*** [IDCARE]

"Artificial intelligence has the potential to facilitate better targeted, more frequent and widespread criminal attacks, and is already being used for password guessing … (it) ***can be tailored to prey on specific vulnerabilities"*** [AIC]

"ASD joined international partners to call out Russia's Federal Security Service's use of 'Snake' malware for cyber espionage, and … a People's Republic of China state-sponsored actor that used 'living-off-the-land' techniques to compromise infrastructure organisations". [ASD]

Blockchain analytics companies – ***"in the ACCC's experience, these organisations are generally unwilling to block or freeze wallets until law enforcement open an investigation, or an extensive assessment has been completed***" [ACCC]

Key challenges to any solution include:

- **extraterritoriality** (which can give the criminals immunity);
- **encryption** (a significant barrier to detection, investigation and prosecution); and
- **cryptocurrencies** (enables criminals to effect instant borderless transfers) [CSCRC]

  > ***The ability for threat actors to move proceeds of crime from traditional banking to cryptocurrency environments is well known This allows the transfer of proceeds seamlessly offshore"*** [IDCARE]

Emerging threats are perceived to include artificial intelligence, and the Internet of all Things (IoT) cybersecurity [CSCRC].

Then there are malicious software called 'infostealers' or 'stealers' – Redline, Raccoon, Mars.

> ***"the most significant concern lies in Infostealer's capacity to circumvent anti-virus solutions and evade endpoint detection and response (EDR) platforms. This poses a major problem as the false negatives triggered may go undetected unless actively and specifically investigated"*** [IDCARE]

The prospects that law enforcement will be able to contain cybercrime and recover losses are the subject of negative expectations:

> ***"… many cybercrimes are likely to grow no matter what law enforcement do about them"*** [CCRT-DU]
>
> ***"Many police agencies are clear that they are unable to assist with recovery of funds when a victim makes a report"*** [AIC]
>
> ***"These capability gaps are amplified by increasingly complex and technologically sophisticated offenders and offences, which also undermine police surveillance and evidence-gathering efforts"*** [AIC]

Some problems faced by police that will constrain and restrict the efficiency and effectiveness of law enforcement appear to include:

> ***"Police organisations tend to view cybercrimes as a 'specialist' domain, yet they*** *largely maintain a 'generalist' ethos to reporting". … It should be clear that specialist units are unable to manage all cybercrime* [CCRT-DU]
>
> The Jurisdictional aspects to detection, investigation and prosecution are complex. Internal and external intelligence sharing within and across those jurisdictions are a challenge. There are often limitations to the timeliness and accessibility of real-time intelligence. Individual and business cyber resiliency … illustrate the challenges of enforcing the law. Barriers to more open sharing from industry include *perceived risk of regulatory action, potential legal action and reputational risk* [IDCARE]
>
> *Entities with the weakest controls, such as certain online-only banks … are disproportionately represented in reports to Scamwatch as the recipients of stolen funds* [ACCC]

A fair summary of the picture painted by the AIC and others may be that there will be multiple victimisations, most not reported, where few reports lead to arrest, and dissatisfaction with police occurs [AIC].

Liability – It may be argued that Insurance companies may be forcing terms and conditions upon banks to load the responsibility for losses caused by internet crime onto owners and operators of the bank accounts, rather than on the banks or on the firms that hold the owners bank information by forcing them into [On-line Only] arrangements.

> Only 2.5 % of fraud & scam victims who lost money were able to recover any of their losses [AIC], and only 2.5% fraud or scam victims were told by police that someone was arrested, charged or prosecuted [AIC]

> ***… institutions on which*** (Australian residents) ***rely … have often failed to implement basic measures to protect their customers, all while carefully drafting terms and conditions and privacy policies designed to protect themselves from legal claims when their customers suffer losses when utilizing their products and services*** [LaC]

> ***Consumers who have spent their lives protected from certain risks under the law do not appreciate that with technological advances some of these legal guardrails have been silently removed or no longer apply*** [LaC]

> ***Contractual arrangements between consumers and technology companies*** (are used) ***whereby tech companies can exclude liability or cap their liability to minimal levels even in the case of negligence or breach of contract*** [LaC]

> ***Many police agencies are clear that they are unable to assist with recovery of funds when a victim makes a report*** [AIC]

> ***Prior to electronic banking, payments of large sums were generally made by cheque. The effect of the Cheques Act is to hold banks liable when they pay out on a fraudulent cheque … however, in the case of electronic banking, which customers have been transitioned to use, the liability of making a payment to the wrong bank account rests instead with the transferor, because they have actively paid the money into the wrong account, even though they may have had no real mechanism for checking that they were paying the money to the correct person or entity*** [LaC]

By comparison, the use of cheques is guided by 300 years of experience of writing legislation, handling disputes and enforcing laws against fraud.

Attraction – It may be argued that most individuals and families are a small economic entity not publicly listed, and are thus too small to attract, directly, the resources for crime applied by rogue nations and protected criminal regimes towards larger organisations.

> ***"… customers continue to bear losses that they have limited ability to prevent"*** [ACCC].

> AIC has offered the summary that cybercrime targeting of Australian computer users '***is extremely lucrative'***. LaC describe Australia as ***a honeypot for cybercriminals***

> ***The ease with which cybercriminals can utilize the banking system to defraud Australians is a significant contributing factor to levels of cybercrime experienced in this country*** [LaC]

> ***… criminals are able to disguise their identity using VPNs, TOR software, cloud-based servers or other mechanisms such as using a network with many users, for example at an airport. Cybercriminals are therefore much harder to identify than those who are guilty of more conventional crimes*** [LaC]

Not all perpetrators are Australians, some of the most damaging cybercrimes have and are being conducted by state sponsored actors from countries allowing the perpetrators immunity [CSCRC]

The cybercrime business model – increasingly a value chain of specialized functions – involves an ecosystem of sophisticated cyber-attacks to monetization through fraud and scam [IDCARE]

Key challenges are extraterritoriality (providing immunity), encryption (significant barrier to detection investigation and prosecution) and cryptocurrencies (instant borderless money transfers) [CSCRC].

Scam emails are almost indistinguishable from human-made equivalents [AGD]

The true number of fraud and scam incidents involving unique victims will be at least 4.5 times the number reported by ReportCyber, according to [AIC]. "***Less than 15% of reports from the community came via ReportCyber or via law enforcement."*** [IDCARE]

Australians reported to Scamwatch $158.3 million losses where cryptocurrency was the payment method. [ACCC]

The impact of these losses is ***"potentially catastrophic"*** [AIC]

Practical impacts include ***"the loss of confidence in the internet"*** [AIC]

The contest between criminals and police is described as ***'this 'Arms race'*** [AIC], but

> ***"One report to ReportCyber every 6 mins – far outweighs the capacity of law*** **enforcement"** [AIC]

And thus the ACCC summarises:
"… customers continue to bear losses that they have limited ability to prevent" [ACCC]

Young people are the most vulnerable to cybercrime (31% aged 18-24) –
"Younger people are more likely to be cybercrime victims" because of ***"more time spent online … for personal use"*** [CSCRC; AIC]. Older people are the second most vulnerable (20.3% of those 65yr and older) [CSCRC].

The recent recommendation by the Australian Federal Police that the elderly get their grandchildren to assist them with On-line management of their finances shows just how out of touch with the dynamics of cybercrime is Australia's principal law enforcement body leading our anti-cybercrime response.

A ***'scambulance test'*** that IDCARE have conducted has reported that ***"… only 9.6% of participants demonstrated sufficient skills and knowledge to detect and prevent scam attempts*** [IDCARE]

And this IDCARE statistic is a calculation for the total Australian population, and is much improved upon the vulnerabilities demonstrated by particular groups within Australia's population, such as with:

- Repeat victims,

  > ***… repeat victims … disproportionately impacted -should be prioritized for intervention"*** [AIC].

- People with a restrictive health condition [AIC];
- First nation cultural practices, [AIC; IDCARE];
- LGB persons [AIC];
- People with a language other than English [AIC; IDCARE];
- Respondents who used various online safety measures had a higher prevalence of cybercrime victimization [AIC];
- Small to medium business owners, operators and managers experience significantly higher rates of all types of cybercrime, as they have not the resources, expertise and capability of larger organisations to prevent cybercrimes [CSCRC; ABA];
- Remote clients suffer more than metropolitan clients;
- Secondary victims of data breaches within business or services with which they deal – there can be … flow-on implications to the customers of such entities [AIC]; and
- Donators to charities (most charities are very small) and volunteer-run organisations. Examples include, the 2020 attack on Save the Children, 2022 attack on The Smith Family, plus the attack on Pareto Phone – the telemarketer at the centre of this charity cyber hack targeted tens of thousands of Australian donors [ACNC].

And IDCARE warns that:

> ***"…support of serious harm cases from ReportCyber and direct from law enforcement will not continue without renewed funding support".***

Summary

We repeat here an impressive building of the facts, statistics, factors, and expert opinions into summary conclusions about the on-line financial transactions system in Australia that has been provided by Law & Cyber. Their submission to the Senate Inquiry into Cybercrime stated that the banking sector has failed to adequately protect consumers from fraud during the change from cheque-based payments to electronic banking. They argue that financial services like banking should be fit for purpose. The observations by this expert in practice, in all areas contributing to the failure, namely:

Legislation –

- banks are allowed to transfer funds to cryptocurrency;
- banks are not required to do name checks;
- technology firms are allowed to set liability caps to minimal levels even in the case of negligence or breach of contract; and

- millions of organisations are allowed to forcibly and / or coercively collect databases of personal information.

Technology –

- technology is enabling fraud more than it is preventing fraud;
- technology is facilitating the deception that underpins vulnerability; and
- technology companies use the option to 'blame people' when people suffer losses, and not blame the ease with which cybercriminals can utilize the banking system to defraud Australians.

These few of the many factors contributing to the failure of the system may be a complete demonstration that the On-line financial transactions system in Australia, and their OFTs, may not be fit for purpose.

APPENDIX B TO
CYBERCRIME AND RISK MITIGATION
DATED AUGUST 2025

SECURITY STRATEGY FOR INDIVIDUALS AND FAMILIES

An individual or family has a reasonable need, in QWAG's view, to devise and follow their/its own cybersecurity plan summarized by the four pillars that follow:

1.Placing the Consumer, at the Centre [CCRT-DU]. We place own risks at the centre of the strategy, not the risks to financial entities. This failure is of their making, by their own design. When we consider whether to use On-line or Off-line methods of operation, we allow ourselves to choose either of the associated OFTs or OPPOs, depending on the assessment of the time vs risk circumstances for the type of transfer (e.g. standing transfers or large single transfers; known entities or 'first-time' entities, etc).

For receiving funds, we can accept the longer time taken with cheques for the diminution of our risks, by negating any opportunity for criminals to follow our transactions into our On-line bank account.

For paying funds, we can accept the longer time taken with cheques for the diminution of our risks, by negating any opportunity for criminals to deflect our payments into their own hands:

> ***"… to advance, 'the system' needs to also acknowledge the needs of the victim … to aid their (and our) detection, protection and response priorities … to our national resilience and response efforts"*** [IDCARE]

2.Privacy is critical [Submission 18: Office of the Australian Information Commissioner – hence 'OAIC'] The determinant of susceptibility to victimization may not be the level of training in cyber operations held by the target, but instead may be the volume of personal information held by others, with or without consent, in the financial transactions 'system', together with the volume of exchanges and transactions made On-line with those holding your personal information – that is:

- it is not the target's skill that protects them in most cases, for the criminals are more skillful in 90.4% of targets; and
- it is the amount of information about the person in the financial transactions 'system' that then determines whether or not they become a target, that is, what protects them or exposes them to targeting:

> ***"The volume … of personal information that is collected by entities, combined with other practices such as profiling, monitoring, tracking and unnecessary retention of data, amplifies privacy & security risks"*** [OAIC]

"Privacy and cyber security are inextricably interwoven …" [OAIC]

"… continue development towards a … program to reduce the need for people to share sensitive personal information with business to access services online" [ABA]**.**

3.We will be held responsible for any losses. Accepting that the weight of responsibility for any scam and fraud is, in the current system and on current figures, 97.5% upon the customer, and 2.5% upon the bank. This reality may not be affected by any law, or by any cyberpolicy of any commercial or service entity.

"… the primary responsibility for preventing breaches, including cybercrime, and protecting data in accordance with the Privacy Act, rests with the entities themselves" [OAIC]

Only **2.5 %** of fraud & scam victims who lost money were able to recover any of their losses [AIC]

"… it is essential that responsibility for cyber security is appropriately aligned … with those that are best positioned to reduce risk" [OAIC].

4.The online system is failing. It is not fit for purpose. Principal aspects of this failure include:

An estimated **$4billion was lost to scams** in 2022 [AGD]

"… customers continue to bear losses that they have limited ability to prevent" [ACCC]

<u>The most educated are the most susceptible</u> – ***"Respondents who used various online safety measures had a higher prevalence of cybercrime victimization"*** [AIC]**.** IDCARE's ***'scambulance test'*** results: ***"… only 9.6% of participants demonstrated sufficient skills and knowledge to detect and prevent scam attempts*** [IDCARE]

"The frequency of cybercrime is also increasing. In 2022-23 there were 94000 cybercrime reports (1 every 6 minutes) which was a 23% increase on the previous year

> ***The ability for threat actors to move proceeds of crime from traditional banking to cryptocurrency environments is well known This allows the transfer of proceeds seamlessly offshore"*** [IDCARE]

Cybercrime is ***"a challenge that resists solutions"***

> ***"the most significant concern lies in Infostealer's capacity to circumvent anti-virus solutions and evade endpoint detection and response (EDR) platforms. This poses a major problem as the false negatives triggered may go undetected unless actively and specifically investigated"*** [IDCARE]

The prospects that law enforcement will be able to contain cybercrime and recover losses are the subject of negative expectations:

> ***"… many cybercrimes are likely to grow no matter what law enforcement do about them"*** [CCRT-DU]
>
> ***"Many police agencies are clear that they are unable to assist with recovery of funds when a victim makes a report"*** [AIC]
>
> ***"These capability gaps are amplified by increasingly complex and technologically sophisticated offenders and offences, which also undermine police surveillance and evidence-gathering efforts"*** [AIC]
>
> ***"One report to ReportCyber every 6 mins – far outweighs the capacity of law*** **enforcement"** [AIC]
>
> ***"These capability gaps are amplified by increasingly complex and technologically sophisticated offenders and offences, which also undermine police surveillance and evidence-gathering efforts"*** [AIC]

The resultant practical impacts of significance on **'online Australia'**, to which our strategy is responding, are:

1. ***"… Australians are acutely aware of the very real risks of cybercrime and are seeking more control over the collection and use of their personal information"*** [OAIC]
2. ***"… loss of confidence in the internet "*** [AIC]

These factors reflect the role played by the human factor and how the human factor ***"extends to the notion of 'usable security' - …designed to be user-centric, inclusive and affordable"*** [CCRT-DU].