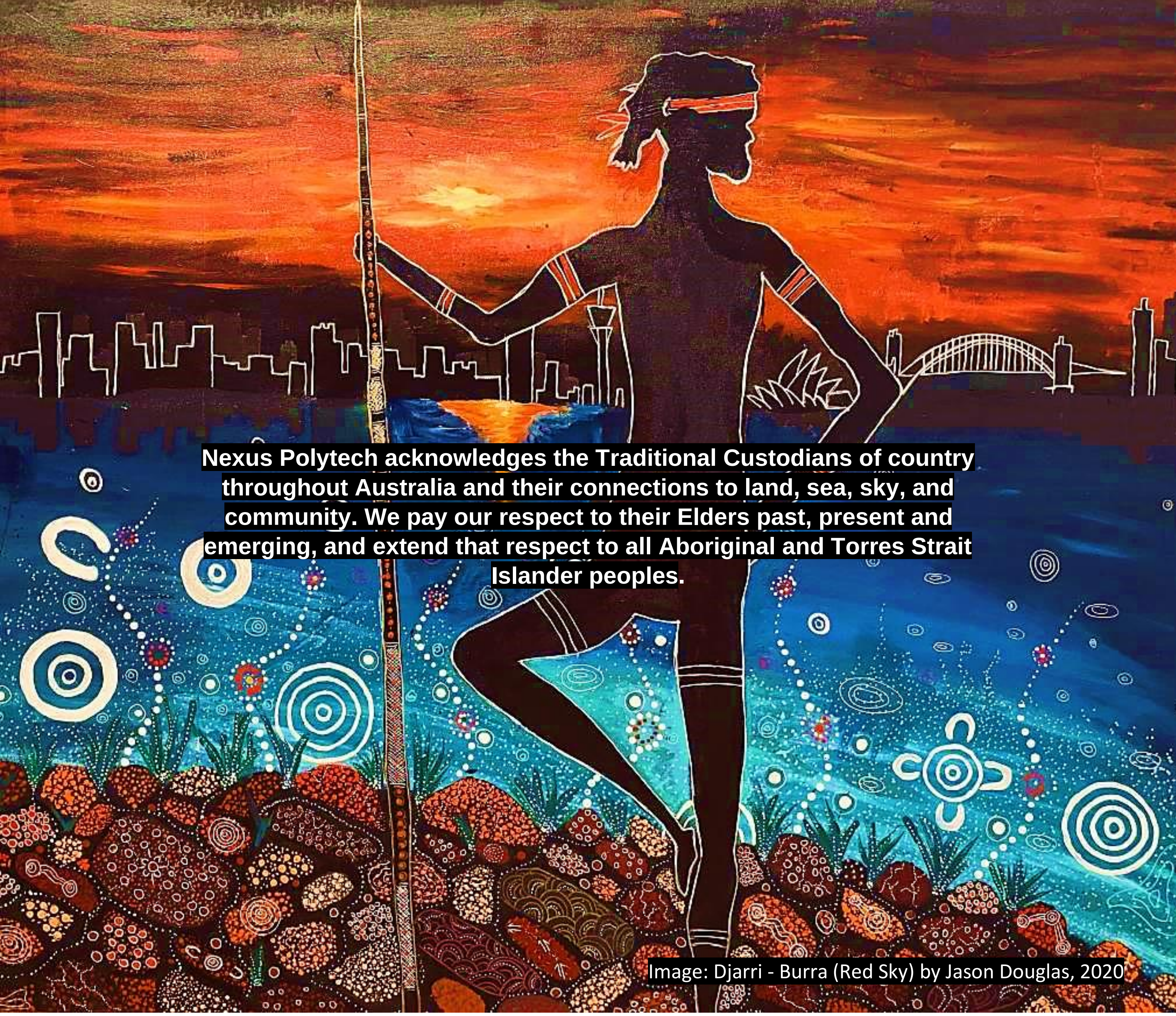
Response to the SMS Sender ID Registry Consultation Paper

20 March 2024

NEXUS POLYTECH



Nexus Polytech acknowledges the Traditional Custodians of country throughout Australia and their connections to land, sea, sky, and community. We pay our respect to their Elders past, present and emerging, and extend that respect to all Aboriginal and Torres Strait Islander peoples.

Image: Djarri - Burra (Red Sky) by Jason Douglas, 2020

This document has undergone a rigorous quality assurance process, where it is assessed to ensure it satisfactorily meets our standards for quality, accuracy, and completeness. Whilst all care has been taken to ensure the accuracy of the contents within this document, it is possible that there may still be errors. If the reader becomes aware of an error or inaccuracy within this document, they should email details of the error to documentservices@nexuspoly.tech.

The author of this document may have used generative AI to assist in crafting its contents. In cases where generative AI has been used, it has been used in accordance with Nexus Polytech’s Artificial Intelligence policy. As such, any generative AI use was ethical and subject to human review and final approval.

The contents of this document are Nexus Polytech's intellectual property and may not be reproduced or distributed without prior consent. Any references or citations to this document should include the publication date and the publishing entity's full name.

www.nexuspoly.tech | contact@nexuspoly.tech | 02 8789 2129

GPO Box 1231 SYDNEY NSW 2001

Contents

Introduction

This is a submission by Nexus Polytech Pty Limited in response to the consultation paper published by the Australian Department of Infrastructure, Transport, Regional Development, Communications and the Arts titled *Fighting SMS Scams - What type of SMS sender ID registry should be introduced in Australia?* on February 2024.

Nexus Polytech is a solutions architecture and consultancy service provider with numerous clients who use alphanumeric sender IDs to communicate with clients via SMS. Nexus Polytech also uses alphanumeric sender IDs in private SMS communication sent from applications to staff for work-related purposes.

The development and implementation of tools, software, and services that use SMS and alphanumeric sender IDs have given us a practical understanding of how businesses use them and the issues, barriers, and limitations associated with them.

An underlying theme in the feedback provided within this submission is leveraging implementations and solutions in other technologies and communication methods. Sender verification and allocation of identifiers is a common issue prevalent in numerous technologies, such as IP addresses, domain names, and email communication. Lessons can be learned from how industry and the wider community responded to these issues through other technologies and implemented inspired solutions to tackle SMS scams.

Executive Summary

Support for a voluntary registration system

We support a voluntary registration system with a blocklist of banned IDs commonly used for scam messages or have a high likelihood of being used by scammers. The voluntary registration model caters for more use cases while protecting users from scams without creating barriers for other legitimate users of alphanumeric sender IDs.

Blocklist for high-risk sender IDs

High-risk sender IDs likely to confuse or mislead users should be blocked, as should generic phrases related to payments. Examples of both include ATO, myGov, Medicare, TaxOffice, Taxation, Centrelink, Bank, Bills, Invoice, and Payment.

Shared and exclusive registration

One particular group of users that needs to be considered are small businesses with a legitimate claim to use a sender ID that is also used legitimately by another business. A voluntary model that permits registration and use of an alphanumeric sender ID by multiple legitimate parties, with the option of exclusive use by a single party for a significantly greater annual fee, would strike an appropriate balance for stakeholders. Big businesses and agencies would have the financial capacity to use their alphanumeric sender ID exclusively and small businesses would be able to use their alphanumeric sender ID with others.

Market-based approach to registering IDs

The implementation of a market-based approach where potential registrants could compete against one another for registration of popular and desired alphanumeric sender IDs, similar to the smartnumbers system from 2004 to 2015 that auctioned 13, 1300 and 1800 numbers, would maximise revenue collected.

Imposing a starting bid would ensure that no sender ID is registered for less than it would been for in a simple pricing structure and allow for a greater degree of access to alphanumeric sender IDs and result in considerably higher licensing fees from competitive purchasers, potentially resulting in lower licensing fee across the board, and greater equality of access to alphanumeric sender IDs for small businesses and not-for-profits.

Protection for rights holders

There needs to be protections for right holders to prevent illegitimate registrants trying to force the legitimate parties to their sender ID from them at a higher value. There also needs to be protections against legitimate registration in bad faith with the sole intent of preventing other eligible parties from being able to register and use that sender ID.

Building on the strengths from other similar Australian registration systems, such as for .au domain names, would strengthen the public's trust in alphanumeric sender IDs and bring consistency across the industry.

Private alphanumeric sender IDs

A small group of alphanumeric sender IDs should be reserved for use by anyone without registration for private purposes. They would need to use generic and precise names to minimise the likelihood of confusion and misuse by bad actors.

The technical limitations of SMS make it an inherently insecure platform

The technical limitations of the SMS protocol mean that the ability to enhance the SMS communication method with security features is unlikely to be implemented in the foreseeable future. As such, many businesses in the banking and financial sectors and government agencies consider SMS an insecure communication method and use secure messaging platforms which only permit legitimate communication between the user and representatives of the business or agency.

Sender verification for SMS

It is technically possible to add a warning label to the body of an SMS, indicating to the recipient that the message may not legitimately be from the sender it claims to be from. Numerous technical considerations need to be resolved in the implementation of such a warning, which are beyond the scope of this submission.

Reporting system for alphanumeric sender ID

A reporting system which reports message claiming to be from the alphanumeric sender ID, including the volume of messages, information about the sender, and details about how the messages were handled, could be implemented for messages sent with alphanumeric sender IDs. This would allow ID owners to collect feedback on how their sender ID is being used and identify potential scams, fraud and misconfiguration.

The contents of the SMS could be included in the report to enable the ID owner to understand the scam campaigns or fraud that is being committed, better educate their users, and exercise preventative and proactive measures.

Adapting to scam and spam trends

As current scamming methods become ineffective, scammers will innovate new techniques to continue preying on victims. With generative acritical intelligence (GenAI) becoming more capable, accessible, and affordable, scammers will use GenAI content to scam unsuspecting victims, increasing their attempts and, unfortunately, their success. Continued education and awareness campaigns remain the last line of defence against scammers.

Questions asked

Question: Do you support the introduction of a voluntary or mandatory SMS Sender ID Registry for alphanumeric sender IDs? Why?

Response: We support a voluntary registration system with a blocklist of banned IDs commonly used for scam messages or have a high likelihood of being used by scammers.

The voluntary registration model caters for more use cases while protecting users from scams without creating barriers for other legitimate users of alphanumeric sender IDs.

One particular group of users that needs to be considered is small businesses with a legitimate claim to use a sender ID that is also used legitimately by another business.

A voluntary model that permits registration and use of an alphanumeric sender ID by multiple legitimate parties, with the option of exclusive use by a single party for a significantly greater annual fee (such as $50,000), would strike an appropriate balance and enable greater flexibility for senders. Users would also have a greater degree of protection as scammers cannot continue their most successful scam campaigns.

High-risk sender IDs likely to confuse or mislead users should be blocked, as should generic phrases related to payments. Examples of both include **ATO**, **myGov**, **Medicare**, **TaxOffice**, **Taxation**, and **Centrelink**, as well as **Bank**, **Bills**, **Invoice, Overdue,** and **Payment.**

It is technically feasible to add a warning label to the body of an SMS, indicating to the recipient that the message may not legitimately be from the sender it claims to be from. Numerous technical considerations need to be resolved in the implementation of such a warning, which are beyond the scope of this submission.

Different use cases have different needs

The use of alphanumeric sender IDs falls into different use cases that have fundamentally different purposes and different needs for the sender. Messages can be classified based on two factors: whether the user consented to receive the message (either expressly or inferred) and if the user solicited the message through a request (directly or indirectly).

Table 1

Categorisation of messages that a user may typically receive.

		Consent Status	
		Consented *(express or inferred)*	**Non-consented**
Solicitation Status	**Unsolicited**	• Alerts • Notifications • Account updates • Direct marketing	• Scam messages • Spam messages
	Solicited	• TOTP codes • Login verifications	

Scam messages are unsolicited messages that the user did not consent to receiving, masquerading as unsolicited messages that they did consent to. For example, scam messages fraudulently claim that the user has made a payment when they have not or have a bill owing when they do not.

Registered sender IDs aim to stop scam messages from masquerading as legitimate alerts and notifications by restricting a sender from using an alphanumeric sender ID that another sender uses. An unintended consequence is that other types of messages, such as alerts and verification messages, may be inadvertently blocked.

Example Use Case 1 – Monitoring Notifications

Polygon Corporation is a business that provides cloud-hosted communication systems to clients. Clients can configure their phones to connect directly to the cloud phone system over the internet and make and receive calls anywhere in the world, with the same experience, no matter where they are.

Servers and network devices are deployed worldwide to run this cloud infrastructure. Special monitoring tools are installed to monitor the health of the servers and devices and report back to the administrators on the health of the services to provide 24/7 uptime.

If a server or device is unresponsive or down, an emergency SMS alert is sent to the system administrators to alert them that there is a problem. This message is sent through various communication methods to several different administrators that are responsible. One of these methods is through SMS, sending a brief description of the alert and using an alphanumeric sender ID of the monitoring server name, which includes the location it is monitoring, such as **SYSMONSYD, SYSMONMEL,** and **SYSMONACT**.

A unique alphanumeric sender ID is used for each location and monitoring service to ensure that notifications are noticed and easily identified by the system administrators as soon as possible so that they can work to restore any degraded services.

Under a mandatory registration system, Polygon Corporation must register a new sender ID for each location they have deployed to or use a single sender ID for all messages and risk critical messages being missed.

<u>Use Case 2 – Small Businesses</u>

There are two small businesses, Partnership Systems Pty Ltd, a software development company located in Hobart, and Partnership Counsellors Pty Ltd, a couples counselling service provider located in Perth.

Both businesses use SMS to communicate with their clients for different reasons. Partnership Systems alert clients when they have overdue payments, and Partnership Counsellors remind patients of upcoming appointments.

Due to the 11-character limit of the alphanumeric Sender ID, both businesses send their SMSs from the sender **PARTNERSHIP**, a name their clients recognise. Neither business can shorten their sender ID or abbreviate it to a name that is recognisable or makes sense to their clients.

Under a mandatory registration implementation, both businesses may want to register the sender ID, but only one could, denying the other use of the sender ID and requiring them to use an alternative.

However, with a voluntary registration system, if the sender ID is not registered, both businesses can use it unless one or another party registers it. Both businesses are supportive of this arrangement as they do not have any shared clients and are permissive of each other (and other legitimate senders) using the sender ID for their messages.

This arrangement would meet the needs of both businesses and allow them to continue sending messages to their clients. However, neither business has any certainty over the continuity of the arrangement as it is contingent on no party registering the sender ID, thus excluding them from being able to use it.

Using the same sender ID for multiple senders

As described in case study 2 above, currently, multiple senders may legitimately use alphanumeric sender IDs. In some instances, the businesses would have no overlapping clients or shared customers and would be permissive of each other using the same sender ID.

A mandatory registration system would prevent any sender from using the sender ID until the first registrant secures it exclusively for themselves. A voluntary registration system would permit all senders to use the sender ID unless/until someone registers it and prevent them from further usage.

Neither option allows small businesses and not-for-profits to use alphanumeric sender IDs, which they may already use for free. Any option that denies legitimate senders from using an alphanumeric sender ID they currently use will lead to communication disruption with clients, increased costs, and inequitable access to the service.

Consideration must be given to how small businesses and not-for-profits can access and use alphanumeric sender IDs equitably.

Many scams use fraudulent alphanumeric sender IDs belonging to or purporting to belong to financial, banking, or government institutions.

A possible option that could merit exploration may be to set the cost for registering an alphanumeric sender ID in a voluntary system to a high price, such as $50,000/year. Registering a sender ID would be prohibitively expensive for any enterprising scammer, but it would be affordable for the rightful owners of sender IDs most used by scammers, such as banks, financial institutions, and the government. This would enable businesses who want exclusive use of a sender ID to register their sender ID, but would not prevent smaller businesses and not-for-profits from continuing to use alphanumeric IDs without registration.

The derivative of this option under a mandatory registration system would be to permit registration and use of a sender ID by any eligible registrant for a low fee, such as $50 a year, and offer the option for a registrant to obtain exclusive use of an alphanumeric sender ID for the high price.

Such an option, or a similar one, would strike a balance and enable greater flexibility for users as they need it. Big businesses and agencies would have the financial capacity to use their alphanumeric sender ID exclusively, small businesses would be able to use their alphanumeric sender ID shared with others, and users would have a greater degree of protection that negates the ability for scammers to use the most popular scam campaigns.

<u>Blocklist for high-risk sender IDs</u>

Implementing a blocklist for sender IDs prohibited from sending messages would be merited. This criterion would capture sender IDs used by government agencies or that could mislead recipients into believing they are from a government agency, such as **ATO**, **myGov**, **Medicare**, **TaxOffice**, **Taxation**, and **Centrelink**.

Sender IDs likely to mislead or misrepresent users in scam attempts include phrases related to payments, such as **Bank**, **Bills**, **Invoice, Overdue,** and **Payment, should also be prohibited.**

New entries would need to be frequently added to the list as scammers find new sender IDs that can mislead or confuse users. This cat-and-mouse game means that the blocklist is a reactive rather than proactive measure. However, it strikes an appropriate balance between protection against scammers and equitable access to alphanumeric sender IDs.

<u>Sender verification for SMS</u>

Due to the proscriptive structure of the SMS message payload specified in the SMS protocol, the maximum data size of the SMS message's data payload is limited. As such, you cannot add additional metadata to an SMS as you would with other communication mediums, such as email.

What is Sender Policy Framework (SPF)?

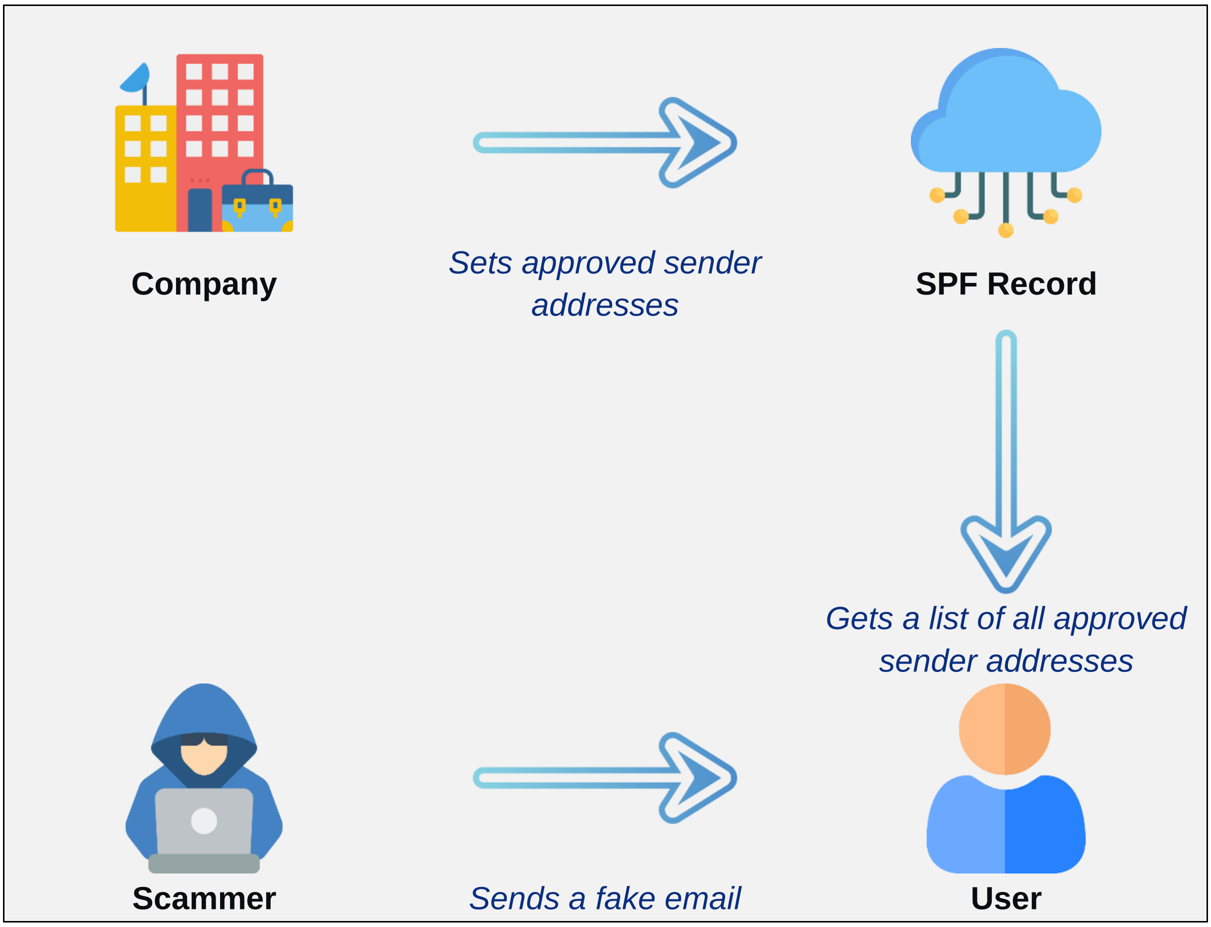
A security mechanism for emails that checks if the sender's address matches an approved list of sender addresses to prevent fake emails from spoofing the From field.

SPF validates the email's supposed sender (using the From field) with data published by the domain of the supposed sender to verify whether this message originated from an approved location.

The result of this validation check is added to the Email header metadata and used to determine whether the message should be sent to Spam/Junk, the Inbox, dropped altogether (when used in conjunction with another email technology called DMARC), or alert the user that this email may not legitimately be from whom it has claimed to be from.

<u>Example</u>

A Scammer sends an email to User spoofing his email address and pretending to be from Company. User’s email client checks the sender of the email address with the SPF record that was published by Company and determines the message sent by Scammer to be fake.


Company
Sets approved sender addresses
SPF Record
Gets a list of all approved sender addresses
Scammer
Sends a fake email
User

A sender verification technique used in email is the Sender Policy Framework (SPF), which adds sender verification data to the Email metadata. While using metadata to indicate if an SMS using an alphanumeric sender ID, or any sender ID for that matter, is valid is preferable, it is unfortunately not technically possible.

As an alternative, the lack of encryption and signing of an SMS data payload means that warning labels can be appended or prepended to the message body of an SMS. This warning label could indicate to the recipient that the message may not legitimately be from the sender it claims to be from.

On a preliminary surface-level evaluation of this approach, two issues need to be considered. The first is countering enterprising scammers who add text to their messages to mitigate the warning label's effect by confusing or misdirecting the user. The second is potential additional costs that may be incurred if the warning text extends the SMS message beyond its maximum length and additional SMSs need to be sent.

It is beyond the scope of this submission to offer any additional remarks on implementing this method. Further consultation with industry and stakeholders would be required.

Question: What, if any, transition arrangements are required?

Response: An essential factor that must be thoroughly considered is ensuring an equitable registration process allowing intellectual property holders to protect their brands and trademarks and enforce their rights.

A method of ensuring equitable access to registration would be through the implementation of a market-based approach where potential registrants could compete against one another for registration of popular and desired sender IDs. A similar system called smartnumbers was implemented from 2004 to 2015 for the registration of 13, 1300 and 1800 telephone numbers.

Protections against misuse, abuse, and malicious use of sender IDs must also exist. This would require a stringent eligibility criterion for registration and a robust dispute process to allow rights holders to enforce their rights. Many lessons can be learned from the administration of .au domain names in this space.

Building on the strengths of the .au eligibility criteria would strengthen the public's trust in alphanumeric sender IDs and bring consistency across the industry, as potential registrants would be familiar with the requirements to obtain and maintain registration.

Similarly, consideration must be given to protecting sender IDs from being registered in bad faith by an eligible party with the intention of preventing its use by another eligible party.

Market-based approach to registering IDs

In instances where numerous parties have a legitimate claim for or interest in an alphanumeric sender ID, a competitive market-based approach should be used to purchase the sender ID to maximise the revenue collected by the registry.

A process based on this principle was the smartnumbers auction system used by the Australian Communications and Media Authority (ACMA) between 2004 to 2015.

The smartnumbers auction system was introduced in 2004 to allocate freephone and local rate numbers (numbers starting with 13, 1300 and 1800) to enable an appropriate return for limited resources. Auctions were conducted fortnightly using an online platform that enabled registered users to list an unregistered number for bidding at the next auction and to see what numbers were available for bidding at the current auction.

In 2014-15, the last year of the system, the ACMA conducted public auctions each fortnight and sold 4,330 numbers, raising approximately $1.66 million in revenue.[1]

A similar system could be used during a time-limited transition period when registration is initially rolled out to allow businesses and agencies to purchase alphanumeric sender IDs, particularly when numerous parties have a claim to register the same sender ID.

This market-based approach would likely see highly desirable sender IDs, which numerous senders could use, attain an initial licensing price far greater than the intended fee in a simple pricing structure. Imposing a starting bid would ensure that no sender ID is registered for less than it would been for in a simple pricing structure.

Overall, a market-based approach would allow for a greater degree of access to alphanumeric sender IDs and result in considerably higher licensing fees from competitive purchasers. This would allow for a lower licensing fee across the board, promoting greater equality of access to alphanumeric sender IDs for small businesses and not-for-profits.

Protection against squatting

Bad faith actors often register names that are an exact or similar match to a business name, brand name, or trademark that they do not have a legitimate claim to, with the intention of forcing the legitimate owner to purchase the name from them at a higher value.

What is Domain Squatting?

Registering domain names similar to existing brands or trademarks to profit from their resale to the rights owner or misdirecting web traffic.

Domain squatting involves registering domain names that are closely related to existing trademarks, popular brands, or commonly searched terms on the internet, with the intention of profiting from them or misdirecting web traffic.

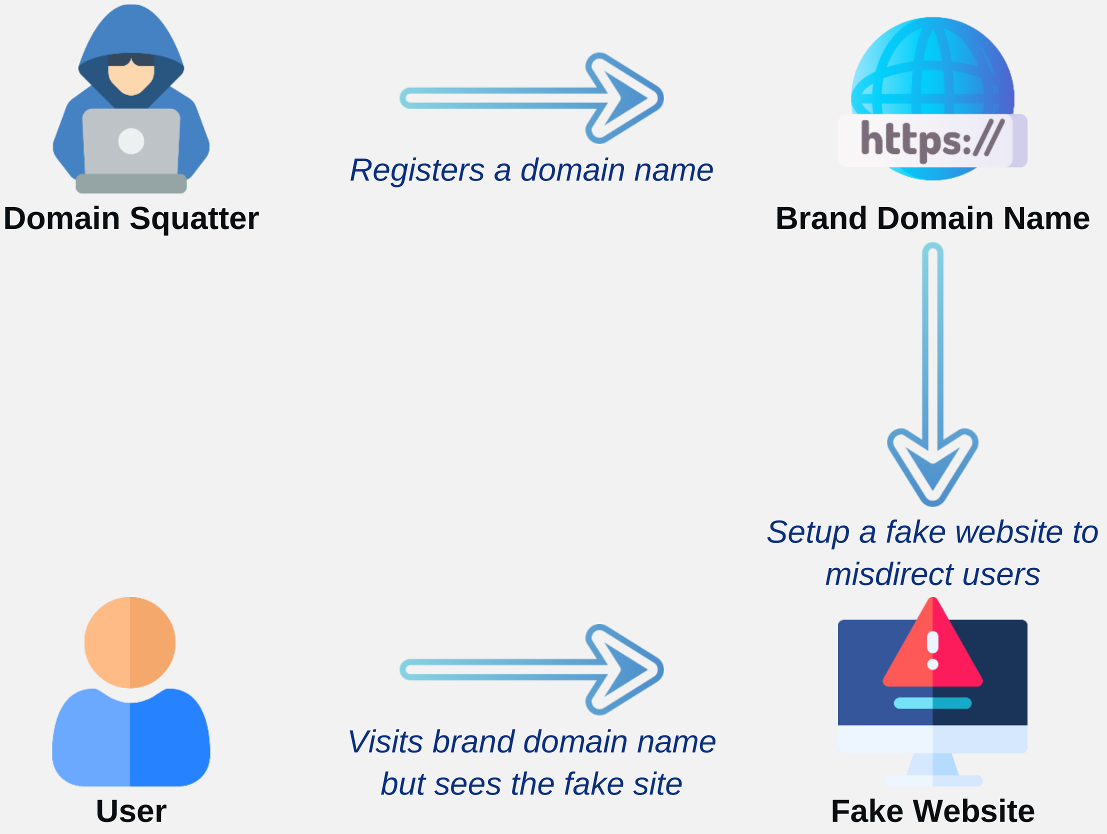
Squatters often anticipate that the rightful owners of these trademarks or brands will eventually want to acquire the corresponding domain names, so they register them first in hopes of selling them back at a much higher price. Alternatively, domain squatters might create websites on these domains filled with ads or misleading content to generate revenue from unsuspecting visitors who mistype or are looking for a legitimate brand's website.

[1] Australian Communications and Media Authority, Communications Report 2014-15

This practice can lead to confusion among consumers and harm the reputation of legitimate businesses, as well as creating lengthy and costly legal disputes over the rightful ownership of the domain name.

Example

A domain squatter registers a domain name that exactly matches a popular brand with the intention of selling it to them at a much higher price. In the meantime, a fake website is set up to redirect traffic to unrelated content, such as advertisements or scams, to profit from the traffic generated by people looking for the legitimate brand website and damage the brand's online reputation to pressure them into purchasing the domain to prevent further harm.


Domain Squatter
Registers a domain name
https://
Brand Domain Name
Setup a fake website to misdirect users
User
Visits brand domain name but sees the fake site
Fake Website

Domain squatting, also known as cybersquatting, is a prevalent issue in generic top-level domain (gTLD) namespaces such as .com, .net, and .org.

In 1999, the international community, through the global multistakeholder group and nonprofit organisation Internet Corporation for Assigned Names and Numbers (ICANN), adopted the Uniform Domain Name Dispute Resolution Policy (the UDRP Policy). The UDRP Policy establishes the legal framework for resolving disputes between a domain name registrant and a third party over abusive registration and use of a domain name in a gTLD namespace.

The World Intellectual Property Organisation (WIPO) has the role of administering the process under the UDRP Policy[2]. In 2023, the WIPO saw a record year in domain name dispute filings, with 6,192[3] cases lodged by trademark owners, a 7% increase from 2022 and a 68% increase since the COVID-19 pandemic.

While the trend indicates that domain squatting is a growing issue on the internet, WIPO data indicates that only 2% of cases filed in 2023 were from Australia. In contrast to gTLD's, domain squatting in the.au Country Code Top-Level Domain (ccTLD) is less prevalent of an issue due to stricter controls and more stringer eligibility and allocation rules for the licencing of domain names.

The .au ccTLD is administered by the .au Domain Administrator (auDA), a not-for-profit organisation established by the Australian internet community to administer and foster a trusted and well-regulated .au ccTLD. Similarly to the UDRP adopted by ICANN, auDA has adopted the .au Dispute Resolution Policy (auDRP), which is an adaptation of the UDRP for the .au namespace.

Table 1

The regulators and entities responsible for ensuring a safe and collaborative internet.

ICANN	.auDA	WIPO WORLD INTELLECTUAL PROPERTY ORGANIZATION
Internet Corporation for Assigned Names and Numbers **(ICANN)**	.au Domain Administrator **(auDA)**	World Intellectual Property Organisation **(WIPO)**
The global multistakeholder group and nonprofit organisation resonsible for coordinating policy on domain name system (DNS) management.	A not-for-profit organisation established by the Australian internet community to administer and foster a trusted and well-regulated .au ccTLD.	A global forum for intellectual property services, policy, and cooperation, administering the Uniform Domain Name Dispute Resolution Policy

[2] World Intellectual Property Organisation, WIPO Guide to the Uniform Domain Name Dispute Resolution Policy

[3] World Intellectual Property Organisation, Record Number of Domain Name Cases filed with WIPO in 2023

The auDRP, in conjunction with auDA's more stringent licencing criteria for domain names, has helped ensure that only people with a legitimate claim to a domain name can register that domain name. Data from auDA on the proceedings brought under the auDRP indicate that only 63 cases were filed in the year 2023[4], with 54% of cases resulting in the domain name being transferred to the rightful trademark owner.

Table 2

Summary of proceedings filed under the .au Dispute Resolution Policy over the last five years.

Year	Total .au Domains	Cases Filed	Cases as % of total .au domains	Transfer Outcomes
2023	4,223,429	63	0.00149%	54.00%
2022	4,160,209	56	0.00135%	55.40%
2021	3,398,583	52	0.00153%	44.23%
2020	3,238,672	43	0.00133%	48.84%
2019	3,171,889	38	0.00120%	47.37%

Data from previous years show an upward trend in the number of cases filed, which is generally consistent with the growth of the .au namespace. Nonetheless, the average number of cases as a percentage of the total domain name space over the last five years remains at an average of 0.00138%, with a dispute rate of 1 per 72,000 domains.

These statistics demonstrate the effectiveness of the .au licensing rules, which use the eligibility criteria to prevent domain squatting, compared to the gTLD namespaces.

There would be merit in drawing on the strengths of the .au eligibility criteria to implement a similar criterion for alphanumeric sender IDs to reduce "ID squatting" and implementing a dispute resolution policy that robustly but fairly allows intellectual property holders the capacity to enforce their rights.

An additional benefit of consistency with the .au licensing rules is the familiarity and experience of businesses and industries. Potential registrants would already be aware of the intellectual property rights required to obtain and uphold a registration of an ID.

Protections against bad faith registration

There are likely to be instances where multiple parties have a legitimate claim to a sender ID and meet the eligibility criteria, and a party that registers a sender ID does

[4] .au Domain Administrator, auDRP Proceedings Database

so in bad faith with the sole intent of preventing the other eligible parties from being able to use that sender ID.

Instances of these situations would not necessarily meet the definition of cybersquatting but may nonetheless prevent intellectual property owners from being able to exercise their rights.

There is benefit in having a process to deal with such claims by eligible rights holders through mediation and arbitration in instances where bad faith can be demonstrated on the part of the registrant. Such claims would necessitate an impartial and expert panel to adjudicate claims and make determinations.

Transparency surrounding this process, including a register of cases, decisions, and decision rationales, would strengthen public confidence in the regulation of alphanumeric sender IDs.

Other Feedback

Alphanumeric sender IDs are also used for private and internal purposes in addition to commercial and public purposes. These private use cases include alerts and notifications from systems such as alarms, monitoring systems and automatic processes. Requiring individuals or businesses to register and pay for alphanumeric sender IDs, which they currently use in private for free, would create an inequitable outcome.

Reserving commonly used and generic alphanumeric sender IDs as private use IDs and allowing anyone to use them without registration strikes an appropriate balance between protecting users and equitable and fair access to sender IDs.

The technical limitations of the SMS protocol mean that the ability to enhance the SMS communication method with security features that handle sender verification, message integrity and authenticity is unlikely to be implemented in the foreseeable future unless significant changes are adopted to the protocol.

Consequently, businesses in the financial services and cybersecurity industries consider SMS an inherently unsafe communication medium. The industry has invested significant resources in developing alternatives to SMS communication and will continue to do so as scam attempts through SMS increase further.

As current scamming methods become ineffective, scammers will innovate new techniques to continue preying on victims. We anticipate an increase in scam attempts made using computer-generated voices engaging in fluid conversations with people through phone calls. Continued education and awareness campaigns remain the last line of defence against scammers.

With generative acritical intelligence (GenAI) becoming more capable, accessible, and affordable, scammers will use GenAI content to scam unsuspecting victims, increasing their attempts and, unfortunately, their success.

Implementing a reporting system for alphanumeric sender IDs would assist ID registrants in better understanding potential fraud and misuse of their IDs. A similar system is implemented in email called Domain-based Message Authentication, Reporting & Conformance (DMARC). DMARC reporting allows the rightful registrant to see the rate of messages being sent with their name from unauthorised sources, who those sources are, and the contents of those messages, allowing them to understand better the scam campaigns or fraud that is being committed and enable them to educate their users better and take preventative and proactive measures.

Private alphanumeric sender IDs

There are use cases where SMS messages sent from alphanumeric sender IDs are used for private purposes other than communicating with clients or with the public. Such use cases could include:

- Time-based One-Time Password (TOTP) codes for verifying logins
- Alerts from monitoring systems such as alarms, sensors and detection systems
- Notifications for automatic systems/software deployment
- Testing software/services that send/ receive SMS with alphanumeric sender IDs

IP addresses, short for Internet Protocol addresses, are unique numerical labels assigned to each device connected to a network. They serve as identifiers for devices such as computers, smartphones, servers, and other networked devices, allowing them to communicate with each other over the network. IP addresses are governed by the Internet Assigned Numbers Authority (IANA).

The vast majority of IP addresses are public, allowing them to be reserved and used by a single device to enable it to send and receive data. However, the IANA has reserved a range of IP addresses designated for use within private networks and not intended to be directly accessible from the internet.

These reserved addresses are classified as private IP addresses and are used for devices within a local network, such as home networks or corporate intranets, to communicate with each other. No one can register these IP addresses for exclusive use as everyone uses them for their own private purposes.

It would be advantageous for a small group of alphanumeric sender IDs to be reserved with a similar classification and intended for use by anyone for private purposes. These private sender IDs would not require registration and would be usable by anyone. They would need to use generic and precise names to minimise the likelihood of confusion and misuse by bad actors.

Table 3

Examples of potential private alphanumeric sender IDs and their intended purpose.

Sender ID	Purpose
MONITORING	Alerts from monitoring systems
ALARM	Messages from alarm systems
CODE	Sending TOTP codes
LOGIN	Used for login related tasks
TEST	Used for testing software/services that send or receive SMS

Technical limitations of the SMS protocol

SMS is an open, industry-standard protocol designed to provide a flexible data communications interface for the transfer of short messages between people and providers. The protocol is designed to be globally interoperable, allowing SMS-capable senders to send messages to any SMS-capable recipient. The message is transferred between various routing entities and message centres before arriving at its destination.

The SMS protocol relies on numerous international technical standards, which impose technical limitations and restrictions on the protocol's operation.

One such limitation imposed by the protocol is the technical restriction on the maximum length of a sender's ID, specifying 15 digits as the maximum length for numeric-only sender IDs (messages from person to person) and 11 characters as the maximum length for alphanumeric sender IDs (known as application-to-person and which are the subject of this consultation paper).

A maximum length of 11 alphanumeric characters (with hyphens and underscores allowed) limits the number of possible sender ID possibilities to 270,511,956,061,751,664 (over 270 quadrillion). Despite this gargantuan number of possibilities, only a tiny subset of combinations are words or names that would be feasible to use as a sender ID.

As such, the limit of 11 alphanumeric characters for a sender ID imposes a genuine restriction on the number of possible options that senders can use. Consideration should be given to ensuring equitable access to sender IDs for small businesses, not-for-profits and startups.

SMS is an inherently insecure communication method

The SMS protocol was initially developed in 1992 and evolved over the years through consensus and significant consultation due to the desire to ensure global interoperability. This meant that while the protocol evolved within the context of mobile telephony technology, it did not necessarily adapt to broader advances in technology and cybersecurity.

One such example of this is that despite being a widely used communication method, the SMS is entirely unencrypted (excluding encryption provided by the signalling protocol), meaning that the messages sent are not protected from being intercepted, read or changed by any third parties involved in the routing and transmission process.

This lack of encryption makes SMS vulnerable to interception by hackers and other malicious actors. SMS messages can be easily intercepted, read, and modified without the need for sophisticated tools. Industry-standard cybersecurity advice is that sensitive information should not be transmitted via SMS as there is no built-in protection to safeguard the messages' contents.

What is a checksum?

A checksum is a unique value calculated from a dataset to ensure its integrity and to detect errors that may have occurred in transmission.

A checksum is a small data set derived from a larger data set that helps detect entry, transmission, or storage errors. Its purpose is to provide a method of error checking and help ensure the integrity of the data.

When data is transmitted, a checksum is calculated at the sender's end and stored within the message. The checksum is calculated again on the receiver's end when the data is received. If the checksums match, it indicates that the data hasn't been corrupted or tampered with. However, if the checksums don't match, it suggests that errors have occurred, prompting the need for data retransmission or error correction.

What is a *cryptographic* checksum?

A cryptographic checksum, also known as a signature or a secure hash, is a unique value of fixed size calculated from a dataset using cryptographic functions.

A cryptographic checksum uses cryptographic algorithms to produce a fixed-size, unique value, known as a secure hash, from a set of data. This hash is designed to be computationally infeasible to reverse-engineer, meaning that even a small change to the input data results in a significantly different hash value.

Secret data only known to the user can be used as input into the cryptographic function to result in a hash tied to the secret data, providing a mechanism to uniquely verify the origin of the data. This type of checksum hash is known as a signature.

Cryptographic checksums are commonly used to verify the integrity and authenticity of data, as even minor alterations to the data will produce a drastically different checksum, making it virtually impossible for an attacker to tamper with the data without detection.

Additionally, the SMS protocol has very few mechanisms built into it to ensure the integrity of the data payload and message contents. While the protocol utilises a checksum to help validate the integrity of the payload and detect transmission errors, this does not protect against a third party modifying the payload and substituting in the new resulting checksum.

In contrast to SMS, email implements numerous mechanisms to ensure authentication, data integrity, and sender verification, such as Sender Policy Framework (SPF), DomainKeys Identified Mail (DKIM), Domain-based Message Authentication, Reporting & Conformance (DMARC), DNS-based Authentication of Named Entities (DANE), and Mail Transfer Agent/Strict Transport Security (MTA-STS) over Transport Layer Security (TLS).

Despite implementing numerous mechanisms, many businesses in the banking and financial sectors and government agencies that deal with finances and payments consider email an insecure communication method due to the risk of scammers and bad actors sending emails with spoofed or similar-looking sender details.

Instead, these businesses and agencies use secure messaging platforms built into their mobile applications and websites, which only permit messages to be sent and received between users and legitimate representatives of the business or agency. SMS and email may be used in circumstances to alert users that they have received a new message and prompt them to log in to the secure platform.

This trend of using secure message platforms exclusively to communicate with clients will only continue as scammers and other bad actors target a greater number of people, and more technically inexperienced users are required to use online banking as more banks transition to digital banking.

Similarly, these businesses also deem SMS to be an insecure platform. Most businesses in the financial services industry that use verification codes to verify clients or transactions invest significant resources in developing code-generating applications such as authenticator applications. This transition is also driven by increased SIM-swapping scams by bad actors. It is important to note that new industry rules introduced by the Australian government in April 2022 mandated multi-factor identification verification before carrying out a high-risk customer transaction such as a SIM swap request.[5]

Adapting to scam and spam trends

Australians reported a record $4.8 billion lost to scams in 2023, representing a 16% decrease over the previous year. As alarming as this figure is, the amount scammed by phishing attempts through SMS messages was $5.4 million in 2023, representing a 39.13% decrease from the previous year.

The data shows several trends, the first of which is that the financial amount lost to phishing scams by SMS has increased by a magnitude since 2021, and the reported number of scam attempts has increased year on year.

[5] Telecommunications Service Provider (Customer Identity Authentication) Determination 2022

Table 4

Phishing scams by SMS message in Australia reported to the ACCC since 2020[6].

	2023	2022	2021	2020
Total scams reported	**301.8** +26.14%▲	**239.2** -16.53%▼	**286.6** +32.64%▲	**216.1**
Total amount lost (million AUD)	**$476.8** -15.97%▼	**$567.4** +75.27%▲	**$323.7** +84.28%▲	**$175.7**
SMS phishing scams	**54,900** +42.90%▲	**38,400** +39.44%▲	**27,600** +112.38%▲	**13,000**
SMS scam loss (million AUD)	**$5.4** -39.13%▼	**$8.8** +2,296.4%▲	**$0.37** -27.17%▼	**$0.29**
Successful SMS phishing scams	1.5%	2.7%	0.5%	**0.8%**

Scammers are opportunistic criminals who seek to prey on people who may not recognise the scam for what it is. They mainly target older people, people from linguistically diverse backgrounds, and people with limited technological literacy. Scammers tend to have a low success rate, with scams reported to ACCC having only a 1.5% success rate. As such, scammers need to make as many attempts as possible to maximise their likely success.

Continued education and awareness campaigns continue to be the last line of defence against scammers. As scam campaigns and methods of scamming become ineffective, scammers will innovate new techniques on new methods and continue to prey on victims.

As generative acritical intelligence (GenAI) becomes more capable, accessible and affordable, there will be an increase in attempts, and unfortunately, success, by scammers who use GenAI content to scam unsuspecting victims. We anticipate that there will be an increase in scam attempts made using generated voices and having fluid conversations with people through phone calls.

As the success rate and capability to scam through one medium, such as SMS, decrease, scammers will move to other platforms. It is important that data continue to be collected and trends evaluated to better understand the effectiveness and impact of anti-scam protections, including the sender ID registry, into the future.

[6] National Anti-Scam Centre, Scam statistics

Lessons from other communication methods

Sender verification and combatting scams and spam are challenges faced by all communication methods to some degree. One method that has an extensive range of control mechanisms to address these issues is email with Domain-based Message Authentication, Reporting, and Conformance (DMARC).

What is DMARC?

An email authentication protocol that prevents spoofing and phishing by enabling domain owners to set policies and receive reports on email authentication results.

Domain-based Message Authentication, Reporting, and Conformance (DMARC) is an email authentication protocol that helps prevent email spoofing and phishing attacks by allowing domain owners to specify policies for incoming email authentication.

With DMARC, domain owners can instruct email providers on how to handle emails that fail authentication checks, such as SPF (Sender Policy Framework) and DKIM (DomainKeys Identified Mail). This can include actions like rejecting, quarantining, or tagging suspicious emails.

Additionally, DMARC provides reporting mechanisms to give domain owners insight into how their domains are being used for email authentication and to monitor and address potential abuse. DMARC reports are feedback mechanisms provided by email receivers (such as email service providers) to domain owners who have implemented DMARC.

These reports provide detailed information about the email traffic claiming to be from the domain owner's domain. DMARC reports typically include data such as the volume of emails received, the authentication results (pass, fail, or none) for SPF (Sender Policy Framework) and DKIM (DomainKeys Identified Mail) checks, information about the sending IP addresses, and details about how the emails were handled (e.g., delivered, quarantined, or rejected).

Domain owners use these reports to monitor the effectiveness of their DMARC policies, identify sources of email abuse or spoofing, and take appropriate actions to enhance email security and authenticity.

A reporting system similar to DMARC reporting could be implemented for SMSs sent with alphanumeric sender IDs that would allow ID owners to collect feedback on how their sender ID is being used and identify potential scams, fraud and misconfiguration.

The contents of the SMS could be included in the report to enable the ID owner to understand the scam campaigns or fraud that is being committed, better educate their users, and exercise preventative and proactive measures.

Nexus Polytech

www.nexuspoly.tech | contact@nexuspoly.tech | 02 8789 2129

GPO Box 1231 SYDNEY NSW 2001