NSW Police Force

Mr Anthony Smith
1A Roma St
SCARBOROUGH QLD 4020

By email: als1969@icloud.com

21 November 2025

Our Ref: GIPAREV-2025-0925657
Your Ref: N/A

Dear Mr Smith

***Government Information (Public Access) Act 2009* (NSW)**
Notice of Decision

1. Original access application

I refer to your access application made under the *Government Information (Public Access) Act 2009* (NSW), (GIPA Act), received on 24 October 2025.

You have applied for access to the following government information relating to responses to representations made by you and further described in the access application:

> *"I request access to the following records created between June 1, 2025, and October 2, 2025 (the date of the Minister's response via Ms. Plibersek's office):*
> *1. Internal Briefings & Memos:*
> ** All internal briefing notes, memorandums, reports, emails or summaries prepared by any unit within the NSW Police Force (including, but not limited to, Kings Cross PAC, Professional Standards Command, Police HQ Ministerial Liaison) for Police Executive, the Commissioner's Office, or the Minister for Police's office regarding my allegations and the representations made by Ms. Plibersek MP and Mr. Greenwich MP (related to F/2025/43622 and F/2025/55291).*
> ** Any documents specifically addressing the status of investigations into my complaints against Issac Rushton, particularly concerning identity theft and the evidence provided (e.g., the Cybertrace report).*
> *2. Source Documentation for Ministerial Claims:*

InfoLink
Office of the General Counsel
Locked Bag 5102 Parramatta NSW 2124
T: 02 8835 6888 **W:** www.police.nsw.gov.au **E:** GIPA@police.nsw.gov.au
TTY: 02 9211 3776 for the hearing and speech impaired ABN 43 408 613 180

** The specific NSW Police Force reports, correspondence, emails or file notes relied upon to advise the Minister that my allegations had been "fully investigated".*
** The specific NSW Police Force documents, assessments, emails or reports concluding there was "insufficient evidence to substantiate claims of identity theft."*
** Records (e.g., COPS/CMFMS entry, officer notes, emails, call logs) documenting the specific interaction where an officer from Kings Cross PAC allegedly "recently spoke with Mr Smith" (prior to the Ministerial responses) and provided "additional information on the outcome of the investigation." (Note: My communication logs indicate formal dismissals, not discussions providing additional information).*
** Internal communications or policy documents justifying the advice to the Minister that I should "contact Kings Cross PAC", despite the known formal communication ban imposed on me by that Command.*
3. Ministerial Correspondence Files:
** Copies of the incoming correspondence from Ms. Plibersek MP (Ref F/2025/43622) and Mr. Greenwich MP (Ref F/2025/55291) as held by the NSW Police Force.*
** Copies of the final outgoing responses (Ministerial Refs MINS-522608304-20911 and MINS-522608304-22693) as held on NSW Police Force files.*
** Any internal NSW Police Force emails or communications tasking units (like Kings Cross PAC) to provide information for these Ministerial responses."*

2. Searches for Information

Under the GIPA Act, NSWPF must conduct reasonable searches to locate the government information you seek.

Having regard to the specific nature of the information requested and the likely location of that information in the agency, the application was sent to the Ministerial and Executive Services unit of the Office of the Commissioner to search for the information you have requested.

Searches were made of the NSWPF electronic Records Management System (RMS), using the references provided in the access application as search terms.

I am satisfied the officers who conducted the searches were provided with the relevant terms of the access application and had the relevant experience to know whether the information applied for was held and how to search for the information.

The result of these searches is set out in the attached schedule.

I am satisfied the agency does not hold any other information falling within the scope of the access application.

3. Decision

I am authorised by the New South Wales Commissioner of Police to determine applications made under Section 9(3) of the GIPA Act.

I have decided under section 58(1)(a) of the GIPA Act, to provide access to some of the information you seek and under section 58(1)(d), to refuse to provide access to some of the information, because there is an overriding public interest against disclosure of the information.

4. Reasons

Under section 9(1) of the GIPA Act, you have a legally enforceable right to access the information you seek, unless there is an overriding public interest against its disclosure.

To determine whether there is an overriding public interest against disclosure of the information I must apply the public interest test.

Section 13 of the GIPA Act sets out the public interest test as follows:

There is an overriding public interest against disclosure of government information for the purposes of this Act if (and only if) there are public interest considerations against disclosure and, on balance, those considerations outweigh the public interest considerations in favour of disclosure.

The public interest test requires that I undertake the following steps:

Step I: identify the public interest considerations in favour of disclosure.

Step II: identify the public interest considerations against disclosure; and

Step III: decide the weight of the public interest considerations in favour of and against disclosure and where the balance between those interests lies.

I Public Interest considerations in favour of disclosure

In accordance with section 12 of the GIPA Act, I have taken into account the following public interest considerations in favour of disclosure of the information:

- The statutory presumption in favour of the disclosure of government information.
- The general right of the public to have access to government information held by the agencies.
- The information could reasonably be expected to inform the public about the operations of agencies and, in particular their policies and practices for dealing with members of the public.
- The information includes your personal information.

II Public Interest considerations against disclosure

When applying the public interest test, the only public interest considerations against disclosure that I can take into account are those set out in the Table to section 14 of, and Schedule 1 to the GIPA Act.

Clause 1(e) of the Table to section 14 provides that there is a public interest consideration against the disclosure of information if disclosure of the information could reasonably be expected to *reveal a deliberation or consultation conducted, or an opinion, advice or recommendation given, in such a way as to prejudice a deliberative process of government or an agency,*

The record the subject of this decision is part of an internal report completed for the purpose of providing advice, opinion and recommendation about the investigation the subject of your correspondence in order to brief the Minister. It was therefore prepared for and taken into account in a deliberative process of the agency.

I note the effect of a public interest consideration is to be assessed at a broad operational level – see *Commissioner of Police, NSW Police Force v Camilleri (GD)* [2012] NSWADTAP 19.

It is to be reasonably expected that officers would be inhibited in recording their candid opinions, advice or recommendations, in relation to such matters if they were aware that a document would be made public. This has been accepted by the NSW Civil and Administrative Tribunal (NCAT) in a number of cases. See for example *Hansen v Commissioner of Police [2020] NSWCATAD 89.*

Officers may also feel reluctant to commit their views in writing and may only feel comfortable participating in deliberations orally. Officers should be free to do in written form what they could otherwise do orally, in circumstances where any oral communication would remain confidential.

Such written communications ensure that a proper record is maintained of the matters considered. If they were to be released for public scrutiny, officers may in the future feel reluctant to make a written record, to the detriment of these processes and the public record. If officials were to be more guarded when giving advice, this would have a damaging effect on the agency's deliberative processes as it would deprive the decision-maker of the relevant information needed to make an appropriate decision.

I am satisfied there is a public interest consideration against disclosure of information under clause 1(e) of the section 14 Table.

Clause 1(f) of the section 14 Table provides that there is a public interest consideration against the disclosure of information if disclosure of the information could reasonably be expected to *prejudice the effective exercise by an agency of the agency's functions.*

As is apparent from the above, the disclosure of the opinions, advice and recommendations provided during the preparation of responses to correspondence would lead to those involved being more circumspect in providing such opinions etc and this would prejudice the effective exercise of the NSW Police Force's functions regarding the provision of information to Ministers and correspondents.

This consideration also applies to the withholding of direct contact details. This information is not publicly available. There is a genuine concern that if this information becomes known, members of the public will attempt to make direct contact with the officer or publish them for the purpose of encouraging other members of the public to 'make contact.

If officers are preoccupied with having to manage large numbers of emails or phone calls from members of the public, they will be diverted from their core functions and for these reasons I am satisfied that the release of direct contact details of officers could reasonably be expected to a prejudice the effective exercise by an agency of the agency's functions.

I am therefore satisfied there is a public interest consideration against disclosure of information under clause 1(f) of the section 14 Table.

Clause 3(a) of the section 14 Table provides that there is a public interest consideration against the disclosure of information that would *reveal an individual's personal information*.

The information withheld under this clause contains information and opinions (of and about other individuals) whose identity is apparent or can be reasonably ascertained from it.

Information that a person expressed a certain opinion falls within the definition of "personal information" either because the information is about the person or because it is the person's opinion about an individual.

The withheld information is therefore personal information as defined in clause 4 of sch 4 to the GIPA Act.

"Reveal" is defined in schedule 4, clause 1 to the GIPA Act to mean to disclose information that has not otherwise been publicly disclosed. *In Commissioner of Police (NSW) v Field* [2016] NSWCATAP 59, the NCAT Appeal Panel held that personal information is only revealed when it is publicly disclosed.

The Appeal Panel in *Field* also decided the definition of personal information was wide and

not defined by reference to matters that have occurred in private but is concerned with information "about an individual". When it comes to the question of whether personal information has been revealed, the statutory provisions are concerned with revealing information, not revealing an event to which the information relates.

In *DQN v University of Sydney* [2019] NSWCATAD 159 (DQN), it was held that even if an applicant is aware of the name of a third party, this information would not be considered to have been 'revealed' where there is no evidence that the information has been publicly disclosed.

In the matter of *Woolley v Lismore City Council* [2013] NSWADT 10, the Tribunal considered that information about the identity of a particular individual would be "revealed" where there was no evidence the information had been "publicly disclosed", despite the fact that the applicant was aware of the individual's identity.

There is no evidence available to me to indicate that the withheld information has been publicly disclosed.

I am satisfied there is a public interest consideration against disclosure of information under clause 3(a) of the section 14 Table.

Clause 3(b) of the section 14 Table provides that there is a public interest consideration against the disclosure of information that would *contravene an information protection principle under the Privacy and Personal Information Protection Act 1998 (PPIPA).*

The information protection principle relevant to this application is that contained in section 18 of the PPIPA, which only allows for disclosure of personal information in certain prescribed circumstances.

Section 18 provides as follows:

> *"**18 Limits on disclosure of personal information***
>
> *(1) A public sector agency that holds personal information must not disclose the information to a person (other than the individual to whom the information relates) or other body, whether or not such other person or body is a public sector agency, unless:*
> *(a) the disclosure is directly related to the purpose for which the information was collected, and the agency disclosing the information has no reason to believe that the individual concerned would object to the disclosure, or*
> *(b) the individual concerned is reasonably likely to have been aware, or has been made aware in accordance with section 10, that information of that kind is usually disclosed to that other person or body, or*
> *(c) the agency believes on reasonable grounds that the disclosure is necessary to prevent or lessen a serious and imminent threat to the life or health of the individual concerned or another person."*

The personal information withheld was recorded by police in the course of their duties.

Disclosure of the personal information in response to an access application under the GIPA Act would not be a disclosure directly related to the purpose for which the information was collected.

There is no basis for the agency to have a reasonable belief that the persons concerned would not object to disclosure.

There is no basis for a reasonable belief that the persons would be aware that their personal

information, could be disclosed in response to an application under the GIPA Act and disclosure is not necessary to prevent or lessen a serious and imminent threat to the life or health of an individual concerned or another person.

Disclosure of personal information in response to your access application would not therefore fall within the scope of any of the disclosures permitted under the terms of section 18.

I am satisfied there is a public interest consideration against disclosure of information under clause 3(b) of the section 14 Table.

III. Balancing the public interest considerations.

I have had regard to the public interest considerations in favour of disclosure of the information as set out above. I have also considered the relevant personal factors of the application, including the motive for making the access application, which I understand to be to know what material informed the content of the correspondence.

I have given some weight to the considerations in favour of disclosure.

On balance, however I give the considerations against disclosure greater weight.

Officials should be able to prepare written material relating to decision-making without hesitation due to fear of disclosure of the material. Officials should be able freely brief the Minister and to put in written form what they could otherwise convey orally, in circumstances where any oral communication would remain confidential. This allows officers to deliberate and make honest and frank recommendations on sensitive matters. It also ensures there is a proper full and retrievable account of deliberations and recommendations available for the record.

There is clearly a public interest in ensuring that there is no prejudice suffered by the agency in exercising its functions which in my view should be given very significant weight when determining the public interest considerations against disclosure in this matter.

Individuals also quite rightly expect government agencies to not reveal confidential information including personal information in response to GIPA information access applications. They should also expect compliance with statutory obligations and the information protection principles. In this regard I note if it were not for the GIPA Act, disclosure of the personal information would otherwise be a breach of the PPIPA.

I have had regard to the fact conditions cannot be imposed on the use or disclosure of information provided in answer to a formal access application.

I have also had regard to the fact that as stated in *Danis v Commissioner of Police, NSW Police Force* [2020] NSWCATAD 138 at [86] disclosure of information in response to an access application under the GIPA Act effectively constitutes disclosure to the world at large.

I am satisfied there are overriding public interest considerations against disclosure of the withheld information as set out above.

5. Review rights

If you are not satisfied with any of the decisions in this notice that are reviewable, you may exercise your review rights under Part 5 of the GIPA Act by requesting:

- an internal review of the decision which must be lodged within 20 working days of the date of this notice, or

- an external review of the decision by the Information Commissioner or the NSW Civil and Administrative Tribunal (NCAT) which must be lodged within 40 working days from the date of this notice.

For further information on your review rights, please visit:

Fact Sheet - Your review rights under the GIPA Act

If you have any enquiries in relation to this decision, please contact me on (02) 8835 6888. In any return correspondence, please quote Our Reference Number stated at the top of this notice.

Yours sincerely

Ian Steptoe

Ian Steptoe
Senior Advisory Officer
InfoLink

SCHEDULE OF DOCUMENTS

InfoLink Page No.	Document Description	Released or Refused	Relevant Public Interest consideration(s) against disclosure: T = Section 14 Table
`1-13	Email – request for response – Plibersek correspondence	Part Released	T1(f)
2-24	Email – Request for advice – Plibersek correspondence	Part Released	T1(f)
25-26	Report – Advice re Plibersek correspondence	Refused	T1(e), T1(f), T3(a), T3(b)
27-103	Annexures to Report – Advice re Plibersek correspondence	Released	N/A
104-105	Email and attachment - Response to Plibersek correspondence	Released	N/A
106-108	Email – request for response – Greenwich correspondence	Part Released	T1(f)
109	Email – Request to State Crime Command (SCC) for advice – Greenwich Correspondence	Part Released	T1(f)
110-111	Report – SCC advice re Greenwich correspondence	Refused	T1(e), T1(f), T3(a), T3(b)
112	Email – Request to Central Metropolitan Region (CMR) for advice – Greenwich Correspondence	Part Released	T1(f)
113-114	Report - CMR advice – Greenwich Correspondence	Refused	T1(e), T1(f), T3(a), T3(b)
115-116	Email and attachment - Response to Greenwich Plibersek correspondence	Released	N/A

Ian Steptoe

From: John-Paul Brookes < T1(f)
Sent: Wednesday, 25 June 2025 13:27
To: #SECRETARIAT
Subject: Minister's response - MINS-522608304-20911 - Tanya Plibersek MP - Anthony Smith - Failure of NSW Police to investigate documented cyberstalking and other matters
Attachments: Cybertrace Investigation - Impersonation and Harassment of Tony Smith - 2025 2.pdf; SMITH Tony.pdf; infographic.html; SMITH Tony.pdf; Bank fraud by Issac Rushton.pdf; scott Tappenden claims Issac is police informant.PDF; Paid drug injection site run from public housing.pdf; DVO Ike Rushton 1 copy.mp4

Follow Up Flag: Follow up
Flag Status: Flagged

OFFICIAL

Hi Team

Can a Minister's response please be prepared in relation to this representation. This relates to MINS-522608304-20424.

Any questions please let me know.

Kind regards

JP

John-Paul Brookes
Departmental Liaison Officer
Office of the Hon Yasmin Catley MP
Minister for Police and Counter-terrorism
Minister for the Hunter

T1(f)

nsw.gov.au

52 Martin Place
Sydney NSW 2000

I acknowledge the traditional custodians of the land and pay respects to Elders past and present. I also acknowledge all the Aboriginal and Torres Strait Islander staff working with NSW Government at this time.

Please consider the environment before printing this email.

OFFICIAL

From: Plibersek, Tanya (MP)
Sent: Wednesday, 25 June 2025 12:44 PM
To: Catley Office Email
Subject: FW: Failure of NSW Police to Investigate Documented Cyberstalking, Impersonation & Drug Trafficking, drug injection clinic in public housing, identity documents production and sale

Dear Minister,

Please find below enquiry and attachments from Anthony Smith of 801/281 Elizabeth St, Sydney.

Kind regards,

Nell

From: Tony Smith <als1969@me.com>
Sent: Wednesday, 25 June 2025 3:33 AM
To: Plibersek, Tanya (MP) <Tanya.Plibersek.MP@aph.gov.au>
Subject: Failure of NSW Police to Investigate Documented Cyberstalking, Impersonation & Drug Trafficking, drug injection clinic in public housing, identity documents production and sale

The Hon. Tanya Plibersek MP - Federal Member for Sydney

Failure of NSW Police Force, specifically officers at Kings Cross Police Station, to investigate a severe and long-running campaign of identity theft, cyberstalking, and criminal impersonation against me.

This situation has been ongoing since 2019. Despite numerous reports and the provision of substantial evidence, no action has been taken against the known perpetrator, Mr. Issac William Rushton.

The criminal conduct includes, but is not limited to:

- The creation of Telegram and other social media accounts in my name to advertise the sale of illicit substances.
- The use of my identity in connection with financial fraud.
- A persistent campaign of online harassment and baiting designed to cause me personal and legal harm.

After being repeatedly dismissed by police, I commissioned an independent forensic investigation by **Cybertrace Pty Ltd.** (report dated 3 June 2025). This report, which I can provide in full, independently corroborates my allegations and provides actionable intelligence, including:

1. Direct evidence of impersonating accounts selling drugs.
2. The capture of the suspect's IP address (**103.53.118.254**) at a specific time and date, linked to the ISP **Swoop/Anycast Holdings**.
3. Confirmation that the suspect registered online accounts using my name.

The failure of NSW Police to act on this credible evidence constitutes a serious dereliction of duty and has left me exposed to significant ongoing risk. It is a clear failure to investigate serious crimes under the *Crimes Act 1900* and the *Crimes (Domestic and Personal Violence) Act 2007*.

I request an urgent and independent investigation into the handling of my case and why NSW Police have failed to pursue these serious, evidence-backed allegations against Mr. Rushton.

I am available to provide the full Cybertrace report and all supporting documentation immediately.

From the report

Subject Telegram Account - @the_real_Tony_smith
https://t.me/The_real_Tony_smith
The bio for this account states:
"**My names Tony and Im an alcoholic.**"
On 21 December 2024 @the_real_Tony_smith stated in the Sydney Party
Lads channel:
"Happy Holidays
[0.5g] $150
[1.0g] $250
[½ 🎱] $400
Another post published by the Subject account in the Sydney Party Lads
Telegram channel stated:
" 🔁 Some updates for you 🔁
✨ Price List ✨
0.25g: $100 🔼 $125
0.50g: $200
1.00g: $350 🔽 $300

1.75g: $450 🔽 $400
3.50g: $900 🔽 $750
If you havent already contacted me through his account @The_real_Tony_smith is where you can access the new price list.
Updates coming soon ➡ SOON
1. Parcel Delivery
2. More Payment Options
3. Rewards & Referral Program”

Given these prices, it was considered highly likely that on the particular
occasions captured by the investigation, the individual operating the
Subject account was purporting to sell cocaine, heroin, or methamphetamines, and not cannabis

Of importance, it is noted that the Microsoft account associated with the
Suspect’s email address, ike.rushton22@gmail.com, is linked to an account
name of Anthony Smith, providing **evidence that he is using the Client’s
identity.**

In terms of civil and tribunal court appearances, the Suspect, in the name
of Issac Rushton, had an extensive record, with **38 attendances listed for
courts in NSW**. "The @the_real_Tony_smith account was identified as being active in the
‘Sydney Party Lads’ Telegram channel, and revealed to be advertising the
sale of illicit substances (cocaine, heroin, or methamphetamines) in
quantities of points, half grams, grams, 1.75 grams and eight-balls.
The @frost_rich Telegram account was identified as being active in the
Sydney Lads Up Late’ Telegram channel, and revealed to be advertising the
sale of ketamine and cannabis, as well as posting about their purported
dark web engagement and potential hacking.

"With likely engagement in the dark

web, **as a trafficker of illicit substances, fraud and other crimes, such**
impersonation might serve the dual function of avenging said conflicts,
and carrying out illicit activity with impunity. **It is therefore vital that law**
enforcement agencies take action to bring due consequences to bear on
the offender, so that he ceases this behaviour.... It is particularly critical that authorities
investigate the matter of the user linked to this IP address who has used
Telegram to promote the sale of narcotics using the name of the Client.”

"Don't meet me (sydney sex pests)" Facebook Group

The direct "address" for this group,.
https://m.facebook.com/groups/364032873189154/.

Issac Rushton, operating under the alias "Ike Rush," is the undeniable creator and administrator of this Facebook group. He's not just a member; he's the one calling the shots, the **sole poster** in this particular group.

2. Group Characteristics and Purpose: The group is classified as a **Public group** and, at one point, had **14 members**. It's openly visible and can be found by anyone.

The group's stated purpose, as per its "About" section, is a **"community for sharing information and experiences about individuals or profiles on Grindr, Scruff, and similar platforms that you might want to steer clear of"**. The sources also indicate it's located in Sydney, Australia, specifically mentioning locations like GLEBE, and POTTS POINT.

3. Content and Activities: Issac uses this group to **publicly "dox" and harass men** who have changed their minds about having sexual encounters with him. The evidence indicates he:

- Posts **private photos and conversations** from dating applications.

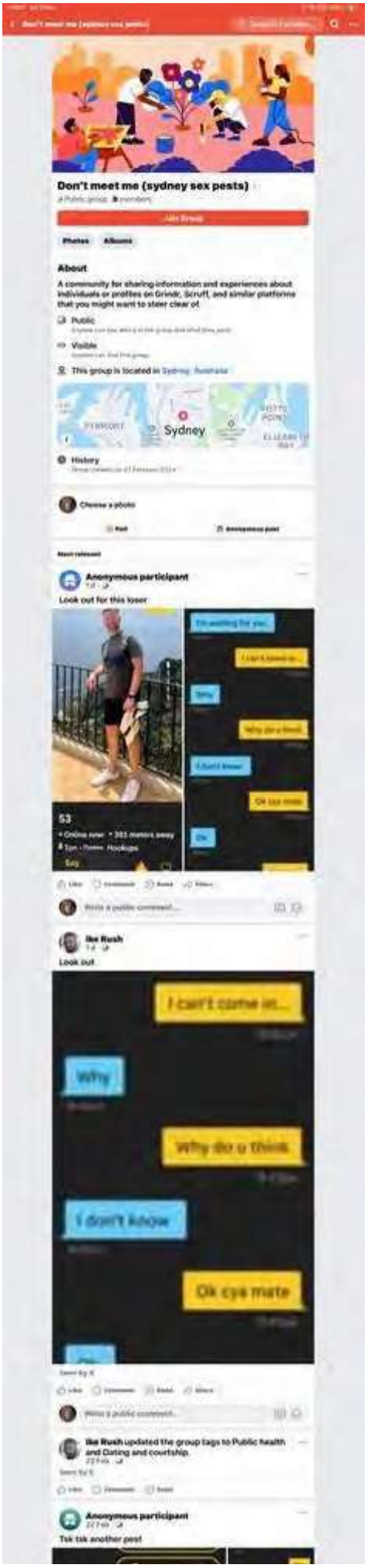
- **Publishes home addresses** and intimate photos of these individuals.
- Labels them with **derogatory names** like "loser" and **homophobic slurs** such as "faggot".
- Actively **encourages further abuse** against these individuals.
- This behavior is explicitly labeled as **sexual violence** and a precursor to physical harm, yet it has reportedly been ignored by police.

4. Specific Incidents and Impact:

- Tony Smith has lodged complaints with police, highlighting this group's abuse, impersonation, and doxing, accusing Kings Cross police of bias and protection of Rushton.
- A specific individual, **Ty Morton, 23 years old**, has had his private photos, address, and entire conversation published online in this group for public ridicule for over a year, and despite attempts, Facebook has not removed the content. Issac reportedly called him a "Faggot" and labeled him a "Loser" for not having sex with him.
- Issac has **no right to an unblemished reputation** given his alleged actions including drug dealing, harassment, impersonation, and inciting suicide, especially when compared to the charges Tony Smith faces.
- The "unredacted posts by Issac are still online" on this platform, meaning the damaging content remains visible.

This group isn't just a digital space; it's an active weapon being wielded, and the evidence points directly to Issac Rushton as its operator and primary aggressor.

.



Tony Smith

0493 998 501

Als1969@icloud.com

801/281 Elizabeth St
Sydney 2000

Ian Steptoe

From: Caroline Shepherd
Sent: Thursday, 26 June 2025 10:01
To: #CMRreturns
Cc: #DCOPMETRO
Subject: Advice request - Tanya Plibersek MP obo Anthony Smith - alleged cyberstalking and misconduct [SEC=OFFICIAL]
Attachments: Cybertrace Investigation - Impersonation and Harassment of Tony Smith - 2025 2.pdf; SMITH Tony.pdf; infographic.html; SMITH Tony.pdf; Bank fraud by Issac Rushton.pdf; scott Tappenden claims Issac is police informant.PDF; Paid drug injection site run from public housing.pdf; DVO Ike Rushton 1 copy.mp4

Importance: High

To	Central Metropolitan Region
Date due to Ministerial and Executive Services	**9 July 2025**
Topic	Lack of police investigation
Correspondent/agency	Tanya Plibersek obo Anthony Smith
Request	Please find attached and below correspondence for review and advice for Ministerial response.
RMS container	F/2025/43622
For more information, please contact	Caroline Shepherd

Thank you

NSW Police Force

Caroline Shepherd
Senior Ministerial Officer
Office of the Commissioner
Locked Bag 5102 Parramatta NSW 2124
E: T1(f) **M:** T1(f)

From: Plibersek, Tanya (MP) <Tanya.Plibersek.MP@aph.gov.au>
Sent: Wednesday, 25 June 2025 12:44 PM
To: Catley Office Email T1(f)
Subject: FW: Failure of NSW Police to Investigate Documented Cyberstalking, Impersonation & Drug Trafficking, drug injection clinic in public housing, identity documents production and sale

Dear Minister,

Please find below enquiry and attachments from Anthony Smith of 801/281 Elizabeth St, Sydney.

Kind regards,

Nell

From: Tony Smith <als1969@me.com>
Sent: Wednesday, 25 June 2025 3:33 AM
To: Plibersek, Tanya (MP) <Tanya.Plibersek.MP@aph.gov.au>
Subject: Failure of NSW Police to Investigate Documented Cyberstalking, Impersonation & Drug Trafficking, drug injection clinic in public housing, identity documents production and sale

The Hon. Tanya Plibersek MP - Federal Member for Sydney

Failure of NSW Police Force, specifically officers at Kings Cross Police Station, to investigate a severe and long-running campaign of identity theft, cyberstalking, and criminal impersonation against me.

This situation has been ongoing since 2019. Despite numerous reports and the provision of substantial evidence, no action has been taken against the known perpetrator, Mr. Issac William Rushton.

The criminal conduct includes, but is not limited to:

- The creation of Telegram and other social media accounts in my name to advertise the sale of illicit substances.
- The use of my identity in connection with financial fraud.
- A persistent campaign of online harassment and baiting designed to cause me personal and legal harm.

After being repeatedly dismissed by police, I commissioned an independent forensic investigation by **Cybertrace Pty Ltd.** (report dated 3 June 2025). This report, which I can provide in full, independently corroborates my allegations and provides actionable intelligence, including:

1. Direct evidence of impersonating accounts selling drugs.
2. The capture of the suspect's IP address (**103.53.118.254**) at a specific time and date, linked to the ISP **Swoop/Anycast Holdings**.
3. Confirmation that the suspect registered online accounts using my name.

The failure of NSW Police to act on this credible evidence constitutes a serious dereliction of duty and has left me exposed to significant ongoing risk. It is a clear failure to investigate serious crimes under the *Crimes Act 1900* and the *Crimes (Domestic and Personal Violence) Act 2007*.

I request an urgent and independent investigation into the handling of my case and why NSW Police have failed to pursue these serious, evidence-backed allegations against Mr. Rushton.

I am available to provide the full Cybertrace report and all supporting documentation immediately.

From the report

Subject Telegram Account - @the_real_Tony_smith
https://t.me/The_real_Tony_smith
The bio for this account states:
"**My names Tony and Im an alcoholic.**"
On 21 December 2024 @the_real_Tony_smith stated in the Sydney Party
Lads channel:
"Happy Holidays
[0.5g] $150
[1.0g] $250
[½ 🎱] $400
Another post published by the Subject account in the Sydney Party Lads
Telegram channel stated:
" 🔁 Some updates for you 🔁
✨ Price List ✨
0.25g: $100 🔺 $125
0.50g: $200
1.00g: $350 🔻 $300
1.75g: $450 🔻 $400
3.50g: $900 🔻 $750
If you havent already contacted me through his account @The_real_Tony_smith is where you can access the new price list.
Updates coming soon ➡ SOON
1. Parcel Delivery
2. More Payment Options
3. Rewards & Referral Program"

Given these prices, it was considered highly likely that on the particular
occasions captured by the investigation, the individual operating the
Subject account was purporting to sell cocaine, heroin, or methamphetamines, and not cannabis

Of importance, it is noted that the Microsoft account associated with the Suspect's email address, ike.rushton22@gmail.com, is linked to an account name of Anthony Smith, providing **evidence that he is using the Client's identity.**

In terms of civil and tribunal court appearances, the Suspect, in the name of Issac Rushton, had an extensive record, with **38 attendances listed for courts in NSW**. "The @the_real_Tony_smith account was identified as being active in the 'Sydney Party Lads' Telegram channel, and revealed to be advertising the sale of illicit substances (cocaine, heroin, or methamphetamines) in quantities of points, half grams, grams, 1.75 grams and eight-balls.
The @frost_rich Telegram account was identified as being active in the Sydney Lads Up Late' Telegram channel, and revealed to be advertising the sale of ketamine and cannabis, as well as posting about their purported dark web engagement and potential hacking.

"With likely engagement in the dark web, **as a trafficker of illicit substances, fraud and other crimes, such impersonation** might serve the dual function of avenging said conflicts, and carrying out illicit activity with impunity. **It is therefore vital that law enforcement agencies take action to bring due consequences to bear on the offender, so that he ceases this behaviour.... It is particularly critical that authorities investigate the matter of the user linked to this IP address who has used Telegram to promote the sale of narcotics using the name of the Client."**

"Don't meet me (sydney sex pests)" Facebook Group

The direct "address" for this group,. https://m.facebook.com/groups/364032873189154/.

Issac Rushton, operating under the alias "Ike Rush," is the undeniable creator and administrator of this Facebook group. He's not just a member; he's the one calling the shots, the **sole poster** in this particular group.

2. Group Characteristics and Purpose: The group is classified as a **Public group** and, at one point, had **14 members**. It's openly visible and can be found by anyone.

The group's stated purpose, as per its "About" section, is a **"community for sharing information and experiences about individuals or profiles on Grindr, Scruff, and similar platforms that you might want to steer clear of"**. The sources also indicate it's located in Sydney, Australia, specifically mentioning locations like GLEBE, and POTTS POINT.

3. Content and Activities: Issac uses this group to **publicly "dox" and harass men** who have changed their minds about having sexual encounters with him. The evidence indicates he:

- Posts **private photos and conversations** from dating applications.
- **Publishes home addresses** and intimate photos of these individuals.
- Labels them with **derogatory names** like "loser" and **homophobic slurs** such as "faggot".
- Actively **encourages further abuse** against these individuals.
- This behavior is explicitly labeled as **sexual violence** and a precursor to physical harm, yet it has reportedly been ignored by police.

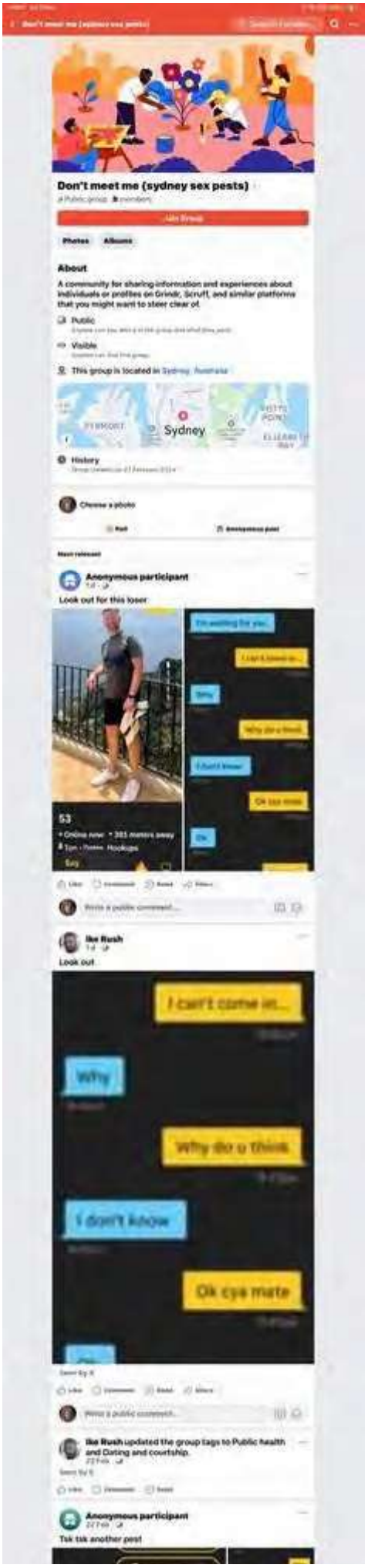
4. Specific Incidents and Impact:

- Tony Smith has lodged complaints with police, highlighting this group's abuse, impersonation, and doxing, accusing Kings Cross police of bias and protection of Rushton.
- A specific individual, **Ty Morton, 23 years old**, has had his private photos, address, and entire conversation published online in this group for public ridicule for over a year, and despite attempts, Facebook has not removed the content. Issac reportedly called him a "Faggot" and labeled him a "Loser" for not having sex with him.

- Issac has **no right to an unblemished reputation** given his alleged actions including drug dealing, harassment, impersonation, and inciting suicide, especially when compared to the charges Tony Smith faces.
- The "unredacted posts by Issac are still online" on this platform, meaning the damaging content remains visible.

This group isn't just a digital space; it's an active weapon being wielded, and the evidence points directly to Issac Rushton as its operator and primary aggressor.

.



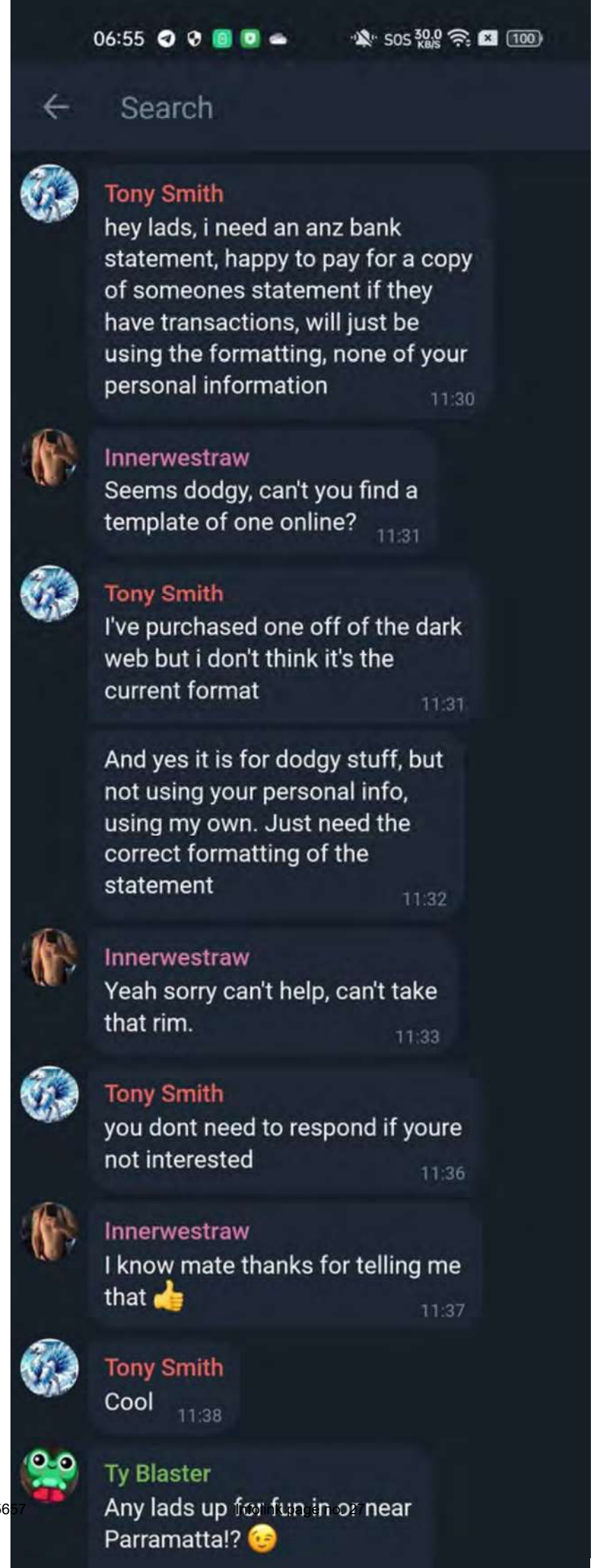
Tony Smith

0493 998 501

Als1969@icloud.com

801/281 Elizabeth St
Sydney 2000

Pages 25 through 26 redacted for the following reasons:
- -
-T1(e), T1(f), T3(a), T3(b)



Cyber Investigation

Tony Smith

Commercial-In-Confidence & Privileged

This report was created for the information of Client, company, and their legal representatives solely on the basis of preparing and assisting in the defence or determination of actual or anticipated legal proceedings. This report must not be copied, reproduced, or transmitted in any manner without the specific written authority of Cybertrace Pty Ltd. Without limitation, this Report does not offer any legal guidance or advice of any kind on any subject. In no event shall Cybertrace Pty Ltd be liable for any damages resulting from, arising out of, or in connection to the use of the information in this report.

CYBERTRACE PTY LTD
ABN: 47 605 834 697
CAPI: 411710138 (NSW)
CYBERTRACE V5 - 2024

Cyber Investigation

Tony Smith

3 June 2025

Our Ref: 2025-4663

Attention: Tony Smith

Dear Tony,

Thank you for your instructions from 7 April 2025. Cybertrace provides you with the following report for your consideration.

Brief: To conduct a cyber investigation with the aim of identifying the individual/s responsible for impersonating, harassing, and cyberstalking the Client.

Contents

Scope of Investigations

As per your instructions, we are completing a proprietary database, technical, open source, and social media investigation with the aim of identifying the individual/s responsible for impersonating, harassing and cyberstalking the Client, Anthony (Tony) Smith.

Extensive investigations, including social engineering combined with custom internal tools, were utilised to identify evidence and intelligence regarding the Subject/s involved. Specific searches were conducted of groups within the Telegram platform, along with analysis of numerous other mobile phone numbers, email addresses, and social media accounts. A background check for the provided Suspect was also conducted.

Background to Investigation

The Client reported that he has been the target of ongoing online impersonation, harassment and cyberstalking through social media and encrypted messaging platforms beginning around 2021. His primary concerns were that an individual and/or their associates were engaging in the following:

- Using multiple alias accounts to monitor, contact, and attempt to provoke the Client into engaging in conduct that could expose him to civil or criminal liability.
- Creating fake accounts impersonating known individuals to manipulate conversations and mislead authorities.
- Making false and defamatory claims to law enforcement and other parties, leading to legal consequences for the Client.
- Being involved in illicit drug distribution and having connections to private online groups where these activities are discussed.

The Client reported that the majority of this offending activity has taken place in groups on the Telegram app. However, Instagram, Facebook and LinkedIn have also been platforms where these activities have occurred.

The Client also provided a screenshot of an exchange from a Telegram group in which an account in the name of Tony Smith asks the other members of the group if anyone can provide an ANZ bank statement so

that he can use its formatting. Another accountholder in the name of Innerwestraw comments:

> *"Seems dodgy, can't you find a template of one online?"*

The account in the name of Tony Smith responds by saying he has purchased one from the dark web which may not be in the current format. The Tony Smith account then goes on to admit:

> *"it is for dodgy stuff"*

(*See appendix*)

It was inferred that this was an attempt at fraud by the individual operating the Tony Smith account, however it was not confirmed whether this particular fraudulent activity was fulfilled.

The Client provided another screenshot of an exchange on an unspecified digital platform between himself and an offending account in which the offender writes in a series of messages to the Client:

> *"Oh my God*
> *You're so pathetic*
> *Why can't you just leave me alone*
> *You're a liar*
> *No one believes you*
> *And you won't ever convince me*
> *So give up*
> *And die already"*

(See appendix)

The Client provided the name of a Suspect, Issac Rushton, as the individual that he believes is responsible for the harassment, defamation and identity fraud, and reported that he is believed to use the aliases of Ike Rush, Tony/Anthony Smith, Zac, Randy Mandan, Randy Gallagher, Randy Sterling and Anthony Hadjakis.

The Client also disclosed that Issac stayed at his house, engaged in an intimate relationship, and by agreement Issac undertook some paid tasks to assist the Client. Following this, a disagreement arose, during and after

which Issac committed multiple offences against the Client. The Client has since engaged legal representation to address these matters.

It is noted that the Client's former legal representative, Hayden Woolf in in an email to the Client on 11 August 2022 referred to Issac as:

> *"...extremely manipulative - sociopathic. Completely self-absorbed. He is a user..."*

The Client provided Cybertrace with numerous phone numbers, email addresses and social media accounts believed to be operated by the Suspect, Issac Rushton. The Client requested that investigations were undertaken to confirm these records as being linked to the Suspect.

The Client also provided legal documents related to the Suspect in which his full name is listed as Issac William Rushton, with a date of birth of 20 December 1988. The Suspect was also linked in provided legal documents to an address of 49 Collins Street, Surrey Hills NSW 2022 prior to a court date on 21 December 2022.

Telegram Investigation

The Client provided the following Subject Telegram accounts:

@frost_rich
@The_real_Tony_smith
@Mr_smitty_au
@the_real_tony_smith_847
@PeetySyd

Due to the way Telegram operates, it was not possible to access content published by specific accounts without being in a shared channel. The Client provided several links and invitations to relevant Telegram channels, three of which were considered of primary interest to the investigation:

Sydney Party Animals ID: 2082543356
Sydney Lads Up Late ID: 1818271742
Sydney Party Lads ID: 2316850399

It is noted that only the accounts @The_real_Tony_smith and @frost_rich were active within these groups at the time of the investigation.

Evidence of numerous posts made by accounts in the name of Tony Smith were captured throughout the course of the investigation, however only those related to potential fraudulent behaviour, dark web operations, and the advertisement of drugs were included in the report. It was considered that other messages that were benign in comparison to the above were less relevant to the investigation, given that the offender could attempt to argue that Tony Smith is a common name. Engaging in fraud, drug trafficking and dark web operations is unlawful irrespective of the name used.

Subject Telegram Account - @the_real_Tony_smith

The Client provided a Telegram account with a username of @the_real_Tony_smith and a display name of Tony Smith for investigation. *(See appendix)*

https://t.me/The_real_Tony_smith

The bio for this account states:

> *"My names Tony and Im an alcoholic."*

This account was reported by the Client to be active in a Telegram channel named 'Sydney Party Lads'.

This channel was joined and observed over a number of weeks to capture evidence of posts published by the Subject, where the following information of interest was identified.

On 21 December 2024 @the_real_Tony_smith stated in the Sydney Party Lads channel:

> *"Happy Holidays*
> *[0.5g] $150*
> *[1.0g] $250*
> *[½ 🎱] $400*
> *[🎱] $750"*

(See appendix)

Another post published by the Subject account in the Sydney Party Lads Telegram channel stated:

"🔄Some updates for you🔄

✨Price List✨

0.25g: $100 🔼 $125
0.50g: $200
1.00g: $350 🔽 $300
1.75g: $450 🔽 $400
3.50g: $900 🔽 $750

If you havent already contacted me through his account ***@The_real_Tony_smith*** *is where you can access the new price list.*

Updates coming soon 🔜
1. Parcel Delivery
2. More Payment Options
3. Rewards & Referral Program"

(See appendix)

Given these prices, it was considered highly likely that on the particular occasions captured by the investigation, the individual operating the Subject account was purporting to sell cocaine, heroin, or methamphetamines, and not cannabis.

Around the middle stage of the investigation, the Subject account left the Sydney Party Lads group.

Other posts made by @the_real_Tony_smith on Telegram were captured, and are not included in this report as they were considered of lesser relevance to the case.

Subject Telegram Account - @frost_rich

The Client provided an account with a username of @frost_rich and a display name of Tony Smith for investigation. The account displays a profile picture of a blue and white cartoon bird. (*See appendix*)

https://t.me/frost_rich

This account was reported by the Client to be active in the 'Sydney Lads Up Late' Telegram channel. The channel's profile picture is an image of two muscular men. The group's description contains the text:

> *"NO SOLICITING OF GOODS AS PER GROUP POLICY Here is the invite only link to this group , qualifications are Sydney Guys who stay up late. https://t.me/+xU33dVp77-wzNzM9 "*

(See appendix)

This channel was joined and observed over a number of weeks to capture evidence of posts published by the Subject, where the following information of interest was identified.

The Subject profile advertised that it could procure cannabis and ketamine, in the following conversation referred to as 'k' and '420':

> dee mcvee: '*Lkn for k and 420....anyone able to get? Alexandria area DM me*'
>
> Tony Smith: '*I can get that on order too*'
>
> ...
>
> Innerwestraw: '*Can you get 420 normally @Au_BigFella*'
>
> Tony Smith: '*I can get what ever within reason, just not for you*'

(See appendix)

The Subject account was further identified as providing advice on cybersecurity to the Sydney Lads Up Late channel and, as part of doing so, also revealed they use the dark web and have software which can be used to hack into accounts. The following post was made by the Subject on 26 July 2024 :

> *"I have the software to bypass screen locks, 2fa, nfc. I use it to learn and protect myself when browsing the ⚫ web. Here's the best tips I can give you.*
>
> *1. Avoid disclosing information in usernames or public facing accuonts names such a telegram for example. Especially avid using your name or date of birth (e.g JohnS89; John Smith born 1989).*
>
> *2. For every layer of security there is a way to bypass or even exploit it. My advice would be to not reply too heavily on cloud or online based security. Depending on methods; its harder to hack a Google account that only can*

be accessed with the password. Having 2 factor enabled in some cases can make it easier to exploit an account.

3. Pay for security; as a consumer you gain guarantees and it is well worth contact out that liability to someone.

4. If you are a victim of fraud and financial institutions can someway confirm that you authorised the transaction (leaving your device unlocked with someone, sharing a one time pass code from your bank, knowing information relating to the disputed charge), you will not give given any assistance. It's always best to answer; 'I don't know'."

(See appendix)

This passage was considered of interest to the investigation as possessing software that can bypass screen locks, two-factor authentication, or NFC security (likely, Near Field Communication) is often viewed as a sign of illegal activity, regardless of the user's stated intent. These tools are typically associated with hacking and unauthorised access, and in many countries, merely owning or distributing them can be a criminal offense under cybercrime laws. While intent is difficult to prove, it was considered possible that the Subject's intent was to use these maliciously, especially when he admits he is using such tools in connection with the dark web; a cyberspace commonly linked to illegal content and behavior.

While cybersecurity professionals may use these kinds of tools legally, they do so within strictly authorised environments. Without such authorisation, using or even having these tools can be interpreted as preparing to commit a crime.

Given the above, it was considered likely that the individual operating the Tony Smith account is very technically savvy. Their advice to people to obscure their identities and lie to banks also indicates amorality, which aligns with the Client's lawyers comments about the Suspect being a sociopath.

The Client also reported that the @frost_rich account, with a display name of Tony Smith, was active in the Telegram channel, Sydney Party Animals.

The Sydney Party Animals group was therefore joined and observed over a number of weeks. In this time the only content posted by the Tony Smith

profile was an advertisement for the Sydney Party Lads Up Late Channel. (*See appendix*)

It is noted that this Sydney Party Animals had an auto-delete feature where all messages older than one week were deleted. Therefore it was considered possible that any offending posts had been deleted before the investigation commenced.

Technical Investigations

A technical tracking link uniquely designed for the purpose of this investigation was created to facilitate the acquisition of the IP address of the user behind the @frost_rich Telegram account. The tracking link was deployed by Cybertrace to the Subject account on the Telegram app at 10:48 (AEST) on 30 April 2025.

Several hostile and commanding messages from the Subject account were received including:

> *"Want to know what James"*
> *"Why dont you pester someone else"*

After the exchange, a message appeared which stated:

> *"Tony Smith uses a self-destruct timer for all chats. All new messages in this chat will be automatically deleted after 1 day they are sent."*

However, the recipient subsequently engaged with the link, without the use of a Virtual Private Network (VPN) or proxy, from an IP address of 103.53.118.254.

Analysis of the IP address 103.53.118.254 was conducted, where it was identified as linked to a location of New South Wales, and an Internet Service Provider (ISP) of Anycast Global Backbone.

Open source searches identified that Anycast provides a method of routing internet traffic, where the same IP address is shared by multiple servers in different locations. When a user tries to connect, the request is automatically sent to the nearest or fastest server available. If one server is too busy, far away, or under attack, the system can redirect traffic to another server.

https://www.cloudflare.com/en-au/learning/cdn/glossary/anycast-network/

Further open source searches identified that Anycast Global Backbone is associated with Anycast Holdings, which has a parent company of Swoop.

https://www.swoop.com.au/

With the provision of the IP address, the date, websites or apps accessed, and times of offending posts, it may be possible for law enforcement agencies to subpoena Swoop in order to obtain data pointing to the offending individual/s. Given the Anycast technology, it will not be as straightforward as identifying an IP address using Unicast technology. However, there are means to determine the links between devices and online activity and ISPs are compelled by Australian law to hold onto the logs of this activity for a minimum of two years after they occur.

Suspect - Issac William Rushton

The Client provided the Suspect as Issac William Rushton, with the following details:

Place of Birth:	Townsville
Date of Birth:	20 December 1988
Current Address:	11/139A Brougham Street, Woolloomooloo NSW 2011
Previous Address:	49 Collins Street, Surrey Hills NSW 2010
Mobile Phone:	Ph +61 474 885 042
Email Address:	ike.rushton@outlook.com

Name Searches

Searches of consumer and investigative databases did not confirm the Suspect as being linked to the provided address of 11/139A Brougham Street, Woolloomooloo NSW 2011. An individual named Russell Symmans was identified as being most recently linked to this address from July 2019

to March 2025, and the property is listed as being currently owned by the Department of Housing.

However, searches of Australian Electoral Commission (AEC) records confirmed that the Suspect is currently enrolled to vote at the provided address of Brougham Street, Woolloomooloo NSW 2011. (*See appendix)*

Searches of consumer and investigative databases did not identify the Suspect as linked to the provided previous address of 49 Collins Street, Surrey Hills NSW 2010. A Thomas Mellor and an Evie Core were linked to this address in 2022.

The Suspect, Issac Rushton, born December 1988 was most recently linked to an address of 207 Lomas Lane, Lovedale NSW 2325 in 2021. No other individuals were identified as being linked to the address at the same time as the Suspect.

Further searches of consumer and investigative databases identified that Issac Rushton, born 1988, was linked to an address of 9 Elberry Crescent, Kelso QLD 4815 in October 2022. Isaac, Kimbra, Jeff, and Stanley Rushton were linked to this address between September 2003 and November 2005, while Stanley, Issac, and Josh Rushton were also linked to the address between July 2017 and March 2023. Property ownership records indicate that this property was purchased by Stanley Joshua Rushton on 23 February 2000, before becoming a long-term rental property, and eventually being sold for $300,000 on 23 April 2020. Given that multiple individuals with the name Rushton were linked to this property, it was considered probable that at one stage this was a family home.

Further searches of consumer and investigative databases identified the Suspect, in the name Issac William Rushton, was also previously linked to an address of 8/1 Cintra Road, Bowen Hills QLD 4006 in May 2007. A Darcy Lynwood Stratford and Jane Louise Corcoran were identified as being linked to the address at the same time as the Suspect.

The Suspect was also identified as linked to Pitt Street, Waterloo NSW 2017 at an unknown date.

Searches of international investigative databases using the Suspect's name identified accounts on the following platforms:

Platforms	Associated Details
BandLab	Username: i_krush Location: Sydney
Pinterest	Username: issacrushton
Soundcloud	soundcloud.com/issac-rushton-390371741 Name: Renters Australia Issac Rushton Location: Sydney, Australia
Github	Username: ikerushton pinterest.com/issacrushton
Skype	Name: Issac Rushton
LiveJournal	hotsta88.livejournal.com/profile
Facebook	https://www.facebook.com/issac.rushton i*****2@gmail.com

Phone Searches

The Client provided a mobile phone number of +61 474 885 042 for the Suspect. Checks confirm this number is currently valid on the Vodafone network. Searches of consumer and investigative databases did not identify any records linked to this number.

Searches were undertaken of international investigative databases, where the mobile phone number was identified as being linked to the Instagram platform. Further technical investigations confirmed that this number is also linked to a Facebook account with a partially revealed email address of i***@******.

Open source searches identified a record listing complaints about this mobile phone number.

https://www.unknownphone.com/phone/0474885042

The record contained six reports by anonymous contributors stating the following about the mobile phone number 0474 885 042:

13 December 2021: *"Just hangs up."*

7 September 2021: *"Voucher book seller*

Call type: Telemarketing"

7 September 2021: *"Online coaching. Pushy"*

6 September 2021: "*Asked for money to support renters"*

5 September 2021: *"Pushy business seeker"*

5 September 2021: *"Donations seeking for own business"*

Further open source searches identified another record listing two one-star ratings for this mobile phone number along with a rating of "Caution" on 13 December 2021.

https://www.telguarder.com/au/number/0474885042

Given the Suspect's known link to tenancy advocacy and coaching, and suspected harassing behaviours, it was considered likely that these were legitimate complaints about his operations. However, as the date the Suspect acquired this mobile phone number is unknown, it was not confirmed that he was responsible for these calls.

Searches of consumer and investigative databases identified a mobile phone number of 0438 537 587 as linked to the Suspect in October 2022. Checks confirmed that this mobile phone number is currently valid on the Telstra network.

Searches of international investigative databases identified that this mobile phone number is linked to various records in the name of Suellen Ribbon, a partial mobile phone number ending in 70 and partial email addresses of s*****n@hotmail.com, w*****e@t*******.com, and w*****0@gmail.com. It was therefore considered highly likely that this mobile phone number had been reallocated to another individual.

Further searches of consumer and investigative databases identified a mobile phone number of 0416 541 318 as linked to the Suspect. Checks confirmed that this mobile phone number is currently valid on the Vodafone network.

Searches of international investigative databases identified that this mobile phone number is linked to accounts on the following platforms:

Platform	Associated Details
CallApp	Saved in another individual's digital contacts as Zac Brissy
EyeCon	Saved in another individual's digital contacts as zack mob
Instagram	Nil
TrueCaller	Saved in another individual's digital contacts as zack mob

Email

The Client provided an email address of ike.rushton@outlook.com for the Suspect. Technical investigations confirmed that the username ike.rushton@outlook.com has been turned off for sign-in, indicating that the Subject uses an alternative method for signing in to this account.

Searches confirmed this email address as being unknown to Australian-based consumer and investigative databases.

Searches of international investigative databases identified this email address as being linked to a Google account with ID 109750812710196980061, which has published four photographs and 14 reviews of establishments in Sydney.

https://www.google.com/maps/contrib/109750812710196980061/

Analysis of these reviews identified a one-star review for Sydney Potts Point Central Hotel, along with a single word, "Scam".

Further analysis of the Google account confirmed that the Suspect had also published a photograph taken at night in December 2021, tagged as Arthur McElhone Reserve. In the photo, an apartment block and its three uppermost apartments are visible, one of which has a light on inside.

Another set of photographs published by the Suspect in June 2021 and tagged as Redfern Park depicts a particular silver hatchback car with a partially visible numberplate of BU 31. (*See appendix*)

Although not confirmed, it was considered possible that these dwellings and the car were linked to an individual/s known to the Suspect, and

therefore that such publication of their possessions and/or whereabouts may be signifiers of stalking and intimidating behaviour by the Suspect.

Searches of international investigative databases identified the email address ike.rushton@outlook.com as linked to accounts on Adobe, Disney, Jotform, Wix, GitHub, Tumblr, Instagram, Snapchat, NextDoor, and Play Games, as well as on the following platforms:

Platform	**Associated Details**
Google	Name: Ike Rushton ID: 109750812710196980061 Device: OPPO Reno4 Z 5G (December 2021) Device: Samsung SM-A205YN (June 2021)
Paypal	Phone: +614 *** 5042 Email: *** on@ou *** .com

Searches of consumer and investigative databases identified an email address of zac20@live.com.au as being linked to the Suspect. Technical investigations confirmed this email address is currently invalid. Searches of international investigative databases identified the email address as only being linked to an account on Nine AU.

Of interest, the email address zac20@live.com.au was also linked in May 2021 to the name Zac Twenty, with a birth date of December 1988, an address of 361/1000 Ann St, Fortitude Valley QLD 4006, and a mobile phone number of 0468 440 334.

S dentified an email a me Issac Rushton. T s not currently valid, and it was not identified as being linked to any other websites, apps, or social media platforms.

Tenancy Database Search

Searches were undertaken of national tenancy databases, where no records were identified in the Suspect's name.

ABN Search

Searches of the Australian Business Registry (ABR) were conducted, where an Australian Business Number (ABN) of 97 351 979 950 was identified for the Suspect in the name Issac Rushton.

The ABN was active from 10 February 2019 to 29 July 2022, and again from 30 March 2024 to current. The Entity Type is listed as Individual/Sole Trader. The ABN was registered for GST from 17 January 2022 to 30 April 2022 and from 6 May 2022 to 28 July 2022.

The main business location was listed as QLD 4306 from 10 February 2019 to 26 August 2020; NSW 2036 from 26 August 2020 to 28 April 2022; NSW 2500 from 28 April 2022 to 30 March 2024; and NSW 2011 from 30 March 2024 to current. No business or trading names were identified as being registered to the ABN.

Domain Search

Reverse domain registrant searches identified the following domain as being registered in the name Issac Rushton on 23 May 2017.

http://evolvealt.org/

Checks confirmed the website www.evolvealt.org is currently inactive. Searches of website archives did not identify any historical copies of the website and no open source records referring to this website were identified.

Further reverse domain registrant searches identified the following domains as being linked to the Suspect's ABN of 97 351 979 950 and the name Ike Rushton:

Domain	Associated Email Address	ABN
parkerrushton.com.au	ike@aussierenters.com.au	97 351 979 950
rentersaustralia.com.au	ike@aussierenters.com.au	97 351 979 950
tenancydispute.com.au	ike@tenantdefence.com.au	97 351 979 950
tenantdefence.com.au	ike@tenantdefence.com.au	97 351 979 950

tenantdefenders.com.au	ike.rushton22@gmail.com	97 351 979 950
tenancydisputes.com.au	ike@tenantdefence.com.au	97 351 979 950

Analysis of these websites confirmed that none are currently active.

Due to these domains being linked to the Suspect's ABN, it is confirmed that the email addresses ike@aussierenters.com.au, ike@tenantdefence.com.au and ike.rushton22@gmail.com are linked to Issac.

Technical investigations confirmed the email address ike@aussierenters.com.au is currently invalid. However, the email address is linked to a Google account, with a partially revealed email address of ike·····@gmail.com and a mobile phone number ending in 42. The Google account has an ID of 100218520543169002211, and has published one rating and three images of Artificer Coffee in Surry Hills NSW.

https://www.google.com/maps/contrib/100218520543169002211/

Technical investigations confirmed the email address ike@tenantdefence.com.au is currently invalid. However, this email address is linked to a Google account, with a partially revealed email address of ike·····@gmail.com and a mobile phone number ending in 42. The Google account has an ID of 112120592326521111137, and has not published any ratings, reviews, or photographs.

https://www.google.com/maps/contrib/112120592326521111137/

Technical investigations confirmed the email address ike.rushton22@gmail.com is currently valid and linked to a partially a partially revealed email address of ike·····@ou·····.com, as well as the mobile phone number 0474 885 042.

The email address is linked to a Google account with an ID of 109750812710196980061, which is noted to be the same Google account linked to the Suspect's email address of ike.rushton@outlook.com.

Searches of international investigative databases identified the email address ike.rushton22@gmail.com as being linked to accounts on OtterAI,

Bitmoji, Spotify, Wix, Jotform, and Facebook. The email address was further identified as being linked to the following accounts and associated details:

Platform	**Associated Details**
Google	Name: Ike Rushton ID: 109750812710196980061 Device: OPPO Reno4 Z 5G (December 2021) Device: Samsung SM-A205YN (June 2021)
LinkedIn	ID: urn:li:person:DgHBYhluqQTNQjtpIWwvWXHZpH-q-9Dsml7y8oeAmLE Name: Mark Eldridge Bio: Building Manager at Central Developments Property Group Location: Sydney URL: linkedin.com/in/mark-eldridge-358772223
Zapier	ID: 9059270
Dropbox	ID: dbid:AACUKWFUW7FG2Y_1V1pgm7hWa6J6BggePos Name: Ike Rushton Profile Picture: *(See appendix)*
Microsoft	ID: E34DAFF5DC3B17AD Name: Anthony Smith Creation Date: 12 November 2024

Technical investigations did not confirm any further contact details linked to the Linkedin account in the name of Mark Eldridge.

linkedin.com/in/mark-eldridge-358772223

Analysis of this account identified that it had no profile picture and that it lists Central Developments Property Group as a place of employment, Full-time Building Manager as profession and Sydney, NSW as a location.

The business name Central Developments Property Group is listed in hypertext, however it does not lead to a separate page. The account follows Forbes and Austrade and has published no further content.

Open source searches of Central Developments Property Group identified that this is a South African company. It was considered possible that this information was fabricated by the Suspect.

Of importance, it is noted that the Microsoft account associated with the Suspect's email address, ike.rushton22@gmail.com, is linked to an account name of Anthony Smith, providing evidence that he is using the Client's identity.

Court Appearance Search

Searches of national civil, tribunal, and criminal court appearance records were conducted, where seven criminal court appearance records with a location of Brisbane were identified in the name of the Suspect, Issac William Rushton. The appearances all occurred between April 2015 and February 2019 at the Brisbane Magistrates Court, Arrest Court (Roma Street) or Ipswich Magistrates Court. Listing types and case numbers were not provided, with the exception of a listing type of Arrests / Remands on 12 February 2019.

Three additional criminal court appearance records were listed in the name of Issac Rushton in Sydney courts. These appearances were considered highly likely to be for the Suspect, given the unique spelling of Issac and that one of these court appearances was an AVO application by the Client against the Suspect. It was further noted that AVO applications were submitted by or on behalf of the Suspect against Thomas M

Unofficial Sex Offender, Domestic Violence, and Child Abuse Registries

Searches were conducted of the Unofficial Australian Sex Offender Registry, which is an online portal that publishes criminal convictions of a sexual nature in Australia, where no records were identified for the Suspect.

Further searches were conducted of an unofficial national database for convicted sex offenders, domestic violence offenders, and child abusers, where no records were identified for the Suspect.

Facebook

Searches of Facebook identified a profile in the name Issac Rushton.

https://www.facebook.com/issac.rushton

Technical investigations confirmed that this email address is linked to a partially revealed email address of i*****2@gmail.com, which aligns with the Suspect's known email address of ike.rushton22@gmail.com.

The profile did not contain a profile or cover picture, had not published any posts, and had not shared any personal information in the About section. Extensive searches did not identify any content published by this profile.

Further searches of Facebook identified a profile in the name Ike Rushton.

https://www.facebook.com/ike.rushton

Technical investigations confirmed that this profile is linked to a partially revealed email address of i*****@i*******.p*******.com.

The profile did not contain a profile or cover picture, had not published any posts, and had not shared any personal information in the About section. Extensive searches did not identify any content published by this profile and it was not confirmed as being linked to the Suspect.

Further searches of Facebook identified a profile in the name Ike Rush.

https://www.facebook.com/i.crush.the.competition

Technical investigations confirmed that this profile is linked to a partially revealed email address of i*****1@gmail.com.

The profile has a profile picture of a bearded man with a back-to-front cap and the cover picture is a banner containing a repeated yellow and black logo containing the letter i (lower case) and an upper case R, very likely signifying the initials of Issac Rushton, the Suspect. (*See appendix*)

It is an open profile with 4000 friends. Information in the Info section indicates that Ike is widowed and has a nickname of Issac. The contact info section provides two links, the first being an Oculus account with the username @I_Krush and a display name of Slaya.

https://www.oculus.com/profile/101525675627101

The other link listed is a YouTube channel in the Suspect's name.

https://www.youtube.com/channel/UCxTtwIq6xInjjI_xVEDyYgA

Searches of the profile identified several posts relating to tenancy and housing issues, with one published on 31 August stating the following:

> *"We established the PR Fund to assist those most vulnerable and at risk of being exploited in their homes.*
> *Donations to the Fund are reserved for tenants that meet eligibility requirements, who without assistance from the Fund, would not be able to access tenant support services.*
> *Who I'm raising money for*
> *Vulnerable tenants without the socio-economic means to access consumer support to best protect their rental agreements at home.*
> *Why I'm raising money*
> *A renter can be anyone, and right now tenants all over Australia need help accessing support to keep them safe at home.*
> *Thank you for supporting vulnerable tenants of Australia"*

(See appendix)

A link was provided in the post to the following fundraiser, where the organisers are listed as Ike Rush and Ann Parker, and the beneficiary is listed as Tenant Defenders. The total amount raised was $50.

https://www.facebook.com/donate/3764212447011830/3764215080344900/

On this fundraising page, the Ike Rush Facebook profile is listed as having been created in 2007. *(See appendix)*

Further searches identified an event created by this profile, named "Issac turns 35". The date of the event is listed as 20 December 2023 and an address of Vale Street, St Kilda is provided.

https://www.facebook.com/events/332600016290838

Searches of the Facebook profile were conducted using the name of the Client, where no records were identified.

Given the creation date of the profile, and links to a fundraising page for Issac's project, his 35th birthday party, and his Oculus and YouTube accounts, it is highly likely that this profile is operated by the Suspect.

Instagram

Searches of Instagram identified an account in the name Issac Rushton.

instagram.com/issac_rushton

Technical investigations confirmed that this account is linked to a partially revealed email address of i****3@h******.au.

The account bio reads:

> *"24 Sydney Uni student, athletic and into having fun* 🤪"

Analysis of this account confirmed that it is locked, and that it has published 21 posts, has 15 followers, and is following 33 other accounts. It was not confirmed that this account is linked to the Suspect.

Further searches of Instagram identified an account with a display name of 'ike rushton'.

www.instagram.com/tenant.defenders

Technical investigations confirmed that this account is linked to a partially revealed mobile phone number of +61*** *** *42 and the partially revealed

email addresses of i*e@t**********.au and i**********1@gmail.com, matching the Suspect's known details.

The profile picture is of a man with dark cropped hair, facial hair, and wearing a purple necktie, who matches the appearance of the individual pictured on the Facebook profile @i.crush.the.competition. The profile has 56 followers and is following 83 other accounts. The bio states:

> *"ike rushton*
> *Personal Coach"*

The only post made by this account was published on 21 July 2021. It is of a room, with a side view of an open oven door, a basin of some sort in the background, and leaves on the floor. There is a hashtag accompanying the post which says:

> *"#rentreduction* 😰"

Given that the technical details align with the mobile phone number and email addresses provided for the Suspect, this Instagram profile was deemed as linked to him.

LinkedIn

A LinkedIn profile was identified in the name Issac Rushton, with a location of Sydney, NSW.

https://www.linkedin.com/in/issac-rushton/

The profile picture consisted of a male matching the appearance of the individual on the @i.crush.the.competition Facebook profile and the Instagram account of @tenant.defenders. This LinkedIn profile picture was noted to contain an 'Open to Work' banner. (*See appendix*)

The profile listed Issac as a Success Coach with a background in customer and consumer services in the real estate industry. The profile also lists experience in communication, management, and leadership, with proficiency in Google Workspace and Microsoft Office. Further listed are services of life coaching, property law, blogging, web development, web design, user experience design, software testing, database development, cloud management, and relocation. Companies listed include Lifebroker in

Melbourne, Evolve ALT in Wellington New Zealand, and Virtual Reality Services.

Technical investigations did not confirm this profile as linked to an email address or mobile phone number.

A second Linkedin account was identified in the name Issac Rushton.

https://www.linkedin.com/in/issac-rushton-6740a792/

(*See appendix*)

The profile lists the Suspect as engaged in Client and Financial Services in the Greater Melbourne area, employed by Lifebroker in Southbank from January 2014 to the present, and as Accounts Receivable at VRS from January 2007 to December 2010. Given that these details align with the other LinkedIn profile, this profile was also considered likely to be linked to the Subject.

Technical investigations confirmed this profile as linked to an email address of issac.rushton@lifebroker.com.au, which was identified as being currently valid.

Open source searches identified that the email address's domain is for a company called Lifebroker Pty Ltd with a website of:

https://www.lifebroker.com.au/

Analysis of this website identified that it is related to an insurance company with a PO Box in Melbourne, VIC.

X (Twitter)

Searches of X (Twitter) identified an account in the name Issac Rushton.

https://x.com/IssacRushton

The account contained a profile picture that matches the Suspect's appearance. No other content was published on this account.

Further searches of X (Twitter) identified an account in the name Ike Rushton.

https://x.com/ike_rushton

This account was identified as joining the platform on 19 November 2019, having no followers and as following one account, Officeworks. The account published three posts on 20 November 2019 about a Officeworks pricematching deal. One of the posts includes a screenshot of an order summary on which a name and address are partially revealed.

... e rushton
... 9 Collins street, Surrey Hills
... URRY HILLS, NSW 2010

(*See appendix*)

Given the Suspect's previous link to this address, this account was deemed to be linked to the Suspect.

Given the date of the account's establishment and that it contacted Officeworks the following day, it was considered highly likely that the account was established for the express purpose of communicating with Officeworks.

YouTube

A YouTube channel was identified in the name Ike Rushton.

https://www.youtube.com/@ikerushton9059

The channel contained four videos on the topic of renters' rights, along with a list of eight links to other social media accounts and websites.

The following links were visited and confirmed as not being valid:

facebook.com/tenantdefence
instagram.com/tenancy.disputes
twitter.com/rentersaus
vm.tiktok.com/ZSJDVBsN9

The remainder of the links were identified as being valid:

1. linkedin.com/company/defenders-tenant

Analysis of this profile confirmed that it is for Renters Australia, which is listed as a civic and social organisation based in Sydney, New South Wales. The Subject is listed as being employed by this company. The profile also lists the organisation as having had between two to ten employees and has maintained a stable headcount of one recorded employee from April 2023 to April 2025. The organisation's median employee tenure is 6.2 years.

2. g.co/kgs/kCc6i8

Analysis of this link identified that it is for a Google search using the terms, NSW Tenancy Dispute Resolution.

3. facebook.com/groups/931393340681530

This link is for a Facebook group named Renters Australia, which has 1.2K likes and 1.3K followers. Its bio states:

> *"Renters Australia is a central info hub for Aussie Renters to learn about their Rental Agreements."*

The group's content pertains to renters' rights and the Admin is listed as the Facebook page Renters Australia, while a moderator is listed as Ann Parker. The Renters Australia page lists a website linked to the Suspect of rentersaustralia.com.au. It is noted that the username of the Renters Australia Facebook page is 'tenantdefenders'.

4. https://open.spotify.com/user/7f8qjvgiuvapuzajqx53xgxk3?si=342881ef816b4bae&nd=1&dlsi=782c09b07d794a4a

Analysis of this link identified that it is a Spotify account with a picture of the Suspect and no further content. An email address of contact@tenancydisputes.com.au was also linked to this account.

Technical investigations confirmed that the email address contact@tenancydisputes.com.au is not currently valid. However, it is linked to a Google account with an ID of 117907779475383223080. Analysis

of the Google account confirmed that the Suspect had not published any ratings, reviews, or photographs.

Searches confirmed the email address contact@tenancydisputes.com.au as unknown to Australian-based consumer and investigative databases.

Searches of international investigative databases did not identify the email address contact@tenancydisputes.com.au as linked to any other websites, apps, or social media accounts.

Advanced Facial Recognition Tools

Extensive reverse image searches were undertaken across several search engines using Facebook and LinkedIn profile pictures of the Suspect, where no further records for the Suspect were identified.

In addition, an advanced facial recognition tool that identifies the image as a query (i.e., search term), and locates images with visually similar elements (colours, textures, patterns, faces etc.) was implemented. The tool scanned websites including publicly accessible pornography sites and blogs, where no images of the Suspect were identified.

Open Source Searches

Open source searches were conducted using the Suspect's names, Issac Rushton and Ike Rushton, where no further relevant records were identified.

Further open source searches were undertaken using the Suspect's name in conjunction with known locations and key terms relating to the investigation such as Sydney, harassment, impersonation, stalking, crime, and drugs, where no records of relevance were identified.

Additional open source searches were conducted using the Suspect's mobile phone numbers, email addresses and aliases, where no records of relevance were identified.

Technical Investigations

A second tracking link, uniquely designed for the purpose of the current investigation was deployed to the Suspect via the email address

contact@tenancydisputes.com.au on 12 May at 16:00 (AEST). The email bounced, suggesting that the email address was not valid at that time.

The same tracking link was then deployed to the Suspect's Facebook profile @i.crush.the.competition via Facebook Messenger on 12 May 2025 at 16:15 (AEST). The Suspect engaged in conversation that was somewhat hostile and commanding, albeit couched in a degree of politeness. It was also noted that the Suspect presented as defensive and cautious when it came to engaging with the tracking link, repeatedly querying the pretext and refusing to cooperate.

All in all, the overall atmosphere of this social engineering conversation was notably similar to the one wherein the initial tracking link to the Subject was deployed, indicating the likelihood that the Subject and Suspect are the same individual.

A third tracking link was deployed to the Suspect on Facebook Messenger to the Don't Meet Me (Sydney Sex Pests) group for which he is an Admin, at 21:42 (AEST) on 21 May 2025. This attempt at engaging was blocked, possibly indicating caution displayed by the Suspect.

An IP address linked to the Suspect was not obtained.

Suspect Email Addresses

The Client provided nine additional email addresses believed to be linked to the Suspect, Isaac Rushton. Investigations were undertaken to identify any evidence that they are being operated by the Suspect.

- slaya@outlook.com.au
- ant.hadjakis@gmail.com
- bjsonoxford@gmail.com
- ike.rushton21@gmail.com
- ike@tenantdefence.com.au
- contact@tenantdefence.com.au
- ike@tenancydisputes.com.au
- ike@rentersaustralia.com.au
- issacrushton@mail.com

slaya@outlook.com.au

Searches confirmed the email address slaya@outlook.com.au as unknown to Australian-based consumer and investigative databases.

Technical investigations confirmed the email address slaya@outlook.com.au is currently valid and linked to a Microsoft account in the name 'mr officer' with a partially revealed email address of ik***@gmail.com.

The email address slaya@outlook.com.au was identified as being linked to a Google account with an ID of 113030570491875685349. Analysis of the Google account confirmed that the Suspect had not published any ratings, reviews, or photographs.

Searches of international investigative databases did not identify any further websites, apps, or social media profiles linked to this email address.

This email address was considered highly likely to be linked to the Suspect due to the usernames of multiple other likely linked accounts containing the word 'slaya' or 'slay', as well as the recovery email address matching the Suspect's known email address.

ant.hadjakis@gmail.com

Searches confirmed the email address ant.hadjakis@gmail.com as unknown to Australian-based consumer and investigative databases.

Initial technical investigations confirmed that the email address ant.hadjakis@gmail.com was linked to a mobile phone number ending in 68 and a Galaxy S24 Ultra mobile phone. It is noted that a mobile phone number of 0451 915 368 provided by the Client as linked to the Suspect on Telegram also ends in 68.

At a later stage of the investigation, it was noted that the email address ant.hadjakis@gmail.com was linked to a mobile phone number ending in 55. It was considered likely that the Suspect changed the account's recovery details during the course of the investigation.

The email address ant.hadjakis@gmail.com was identified as being linked to a Google account with ID 112958275820778747362, which had not published any ratings, reviews, or photographs.

Searches of international investigative databases identified that the email address ant.hadjakis@gmail.com was linked to accounts with Firefox, Adobe, Instagram, Zapier, Facebook, Wix, Github, and Fiverr, as well as accounts on the following platforms:

Platform	Associated Details
Apple	Mobile Phone: **** *** *55
PayPal	Mobile Phone: +614 *** 5368 Email: ***is@gm***.com
Microsoft	ID: 492851360DA739A4 Name: Anthony Hadjakis

It was not confirmed that this email address is linked to the Suspect.

bjsonoxford@gmail.com

Searches confirmed the email address bjsonoxford@gmail.com as unknown to Australian-based consumer and investigative databases.

Technical investigations did not confirm a mobile phone number or email address linked to this account.

The email address bjsonoxford@gmail.com was linked to a Google account with an ID of 104939340287271822704, which had not published any ratings, reviews, or photographs.

Searches of international investigative databases identified this email address as being linked to an account on Spotify.

It was not confirmed that this email address is linked to the Suspect.

ike.rushton21@gmail.com

Searches confirmed the email address ike.rushton21@gmail.com as unknown to Australian-based consumer and investigative databases.

Technical investigations initially confirmed that the email address ike.rushton21@gmail.com was linked to two mobile phone numbers, ending in 55 and 42, matching the details linked to several other accounts belonging to the Suspect.

At a subsequent stage in the investigation, it was confirmed that only the mobile phone number ending in 42 was linked to this email address. It was considered probable that the security settings were changed during this time.

The email address was linked to a Google account in the name Issac Rushton, with ID 112937709804614574754. Although Issac is listed as a Local Guide Level 6 with 4453 points, no reviews or photos were visible.

Searches of international investigative databases identified that the email address ike.rushton21@gmail.com was linked to accounts with Firefox, Adobe, Bose, Deliveroo, Dropbox, Flickr, Instagram, MeWe, Plex, Flickr and Spotify.

Further technical investigations confirmed that the email address ike.rushton21@gmail.com is linked to a Facebook profile with another partially revealed email address of i*****@t**********c*******.

It was considered highly likely that this email address is linked to the Suspect due to the associated recovery details.

ike@tenantdefence.com.au

Searches confirmed the email address ike@tenantdefence.com.au as unknown to Australian-based consumer and investigative databases.

Technical investigations confirmed the email address ike@tenantdefence.com.au is currently invalid. However, it is linked to a Google account in the name 'ike' with an ID of 112120592326521111137. This account is linked to a partially revealed email address of ike·····@gmail.com and a mobile phone number ending in 42. This email account has not published any ratings, reviews, or photographs.

Searches of international investigative databases identified that the email address was linked to accounts with Trello, Adobe, DropBox, and Instagram.

Given that the Suspect's ABN was used to register the domain tenantdefence.com.au it is considered highly likely that this email address was operated by the Suspect.

contact@tenantdefence.com.au

Searches confirmed the email address contact@tenantdefence.com.au as unknown to Australian-based consumer and investigative databases.

Technical investigations confirmed the email address contact@tenantdefence.com.au is currently invalid.

Searches of international investigative databases did not identify this email address as linked to websites, apps, or social media platforms. Specific searches confirmed that it is not linked to a Google account.

Given that the Suspect's ABN was used to register the domain tenantdefence.com.au it is considered highly likely that this email address was operated by the Suspect.

ike@tenancydisputes.com.au

Searches confirmed the email address ike@tenancydisputes.com.au as unknown to Australian-based consumer and investigative databases.

Technical investigations confirmed the email address ike@tenancydisputes.com.au is currently invalid. However, searches of international investigative databases identified that the email address was linked to a Google account with an ID of 100218520543169002211. Analysis of the Google account confirmed that the Suspect had published a single one-star review of a cafe in Sydney called Artificer Coffee in 2022.

https://www.google.com/maps/contrib/100218520543169002211/

Given that the Suspect's ABN was used to register the domain tenancydisputes.com.au it is considered highly likely that this email address was operated by the Suspect.

ike@rentersaustralia.com.au

Searches confirmed the email address ike@rentersaustralia.com.au as unknown to Australian-based consumer and investigative databases.

Technical investigations confirmed this email address is currently invalid. However, it was confirmed as being linked to the same Google account as ike@tenancydisputes.com.au, with ID 100218520543169002211.

Searches of international investigative databases identified this email address as being linked to a mobile phone model of Samsung SM S901E. Also linked to this email address are accounts with Jotform and Spotify.

Given that the Suspect's ABN was used to register the domains rentersaustralia.com.au and tenancydisputes.com.au, it is considered highly likely that this email address was operated by the Suspect.

issacrushton@mail.com

Searches of consumer and investigative databases did not identify any records associated with the email address issacrushton@mail.com. Technical investigations confirmed that this email address is not currently valid.

Searches of international investigative databases identified that the email address issacrushton@mail.com is linked to a Facebook profile which has a partial email address of i*****n@yahoo.com and an eleven-digit mobile phone number ending in 60. The email address is also linked to a FireFox account and a Microsoft account in the name of issac rushton with a location of the US. Given that this mobile phone number appeared to be from a country other than Australia and the location of US was listed with the Microsoft account, it was considered possible that this account was either set up by the Suspect while abroad or linked to another individual of the same name.

Further searches of international investigative databases identified an email address of issacrushton@yahoo.com as linked to the name Issac Rushton. Technical investigations confirmed that this email address was linked to a partial email address of i*****on@gmail.com and a partial mobile phone number of 9*******60.

Attempts at deriving an email address from the partial details of i*****on@gmail.com were made, where an email address of issacrushton@gmail.com was identified as being valid. Technical investigations confirmed that this email address is linked to a partial mobile phone number of 9*******60. The email address was also identified as being linked to a Google account with an ID of 105792571569005904783, which had published one review for an establishment in Canada.

Searches of Facebook identified a profile in the name Issac Rushton.

https://www.facebook.com/ziggy2016

Technical investigations confirmed that this Facebook profile is linked to a mobile phone number ending in 60.

Analysis of its content confirmed that this individual is Facebook friends with other individuals with the same surname, one of whom, Chris Rushton, is listed as linked to Truro, Nova Scotia (Canada).

It was therefore deemed that the email addresses issacrushton@gmail.com, issacrushton@yahoo.com and issacrushton@mail.com are not linked to the Suspect.

Subject Mobile Phone Numbers

The Client provided the following mobile phone numbers as being possibly linked to the Suspect, Issac Rushton. Investigations were undertaken to identify any evidence that they are being operated by the Suspect.

0430 426 201

Searches of consumer and investigative databases did not identify any records for the provided mobile phone number of 0430 426 201. However, checks confirmed the mobile phone number is currently valid on the Vodafone network.

Searches were undertaken of international investigative databases, where the mobile phone number was not identified as linked to any websites, apps, or social media platforms.

Open source searches did not identify any records of relevance associated with this number and it was not confirmed as being linked to the Suspect.

0451 096 509

Searches of consumer and investigative databases identified that the provided mobile phone number, 0451 096 509, was most recently linked to an individual named Linda Smith in November 2021.

Searches were undertaken of international investigative databases, where the mobile phone number was not identified as linked to any websites, apps, or social media platforms.

Open source searches did not identify any records of relevance associated with this number and it was not confirmed as being linked to the Suspect.

0451 915 368

The Client reported that this mobile number was linked to the Suspect on Telegram.

Searches confirmed the mobile phone number of 0451 915 368 as being unknown to consumer and investigative databases. Checks confirmed that this mobile phone number is not valid on any mobile phone networks.

Searches of international investigative databases confirmed that this mobile phone is linked to an account with Whatsapp.

Open source searches did not identify any records of relevance associated with this number and it was not confirmed that this mobile phone number is linked to the Suspect.

Subject Facebook Profiles

The Client provided five active Facebook profiles and one Facebook page that he believed were linked to the Suspect. One of the accounts, with a display name of Ike Rush, was analysed above, and considered highly likely to belong to the Suspect.

www.facebook.com/i.crush.the.competition

Anthony Hadjakis

www.facebook.com/profile.php?id=615587310013l3&_rdr

Technical investigations confirmed that this profile is linked to a partially revealed email address of a*****s@gmail.com. It is considered possible that the full email address linked to this account is ant.hadjakis@gmail.com.

The profile was locked, meaning the published content was not publicly available. It contained a profile picture of a neon crown and no cover picture. Two accounts, Ludovic Bernadat and Luke Cornish, were being followed by the profile.

Searches of Facebook identified the profile as being a member of the Facebook group 'Australia 🇦🇺 Backpackers 2025', where it did not appear to have published any content.

https://www.facebook.com/groups/1154426041280477/

Searches of this profile were conducted using the name of the Client, where no records were identified.

It was not confirmed that this profile is linked to the Suspect.

Anthony Smith

www.facebook.com/profile.php?id=100091242353577

Technical investigations did not confirm any mobile phone numbers or email addresses linked to this profile.

The profile is blank and does not contain a profile or cover picture. Information in the Intro section indicates that this individual lives in Sydney, Australia. Extensive searches of the profile did not identify any other relevant content.

It was not confirmed that this profile is linked to the Suspect.

Karen Thorne

www.facebook.com/karen.thorne.7

Technical investigations confirmed that this profile is linked to a partially revealed email address of c*****2@o**********c*******, as well as three mobile phone numbers ending in 02, 55, and 42.

The profile picture is of crocheted flowers and the cover picture shows a psychedelic image possibly depicting a scene from Alice in Wonderland. Information in the About section indicates that Karen is from Sydney Australia, previously lived in Bardia NSW, and is single. Numerous reviews for cleaning, takeaway food, music education, scrapbooking, and housing services located in VIC and NSW have been published by this account.

The most recent post was a temporary profile picture consisting of a bitmoji character wearing a cat-ear headband and glasses, published on 11 April 2020. (*See appendix*)

Analysis of the interactions with the profile revealed numerous friends who appear to be legitimate individuals.

Searches of consumer and investigative databases identified a Karen Thorne as linked to addresses in Bardia and Dubbo NSW, with the email addresses of coolkids12@outlook.com and coolkids12@optusnet.com.au and a mobile phone number ending in 44. Checks confirmed the email address coolkids12@optusnet.com.au is linked to a Facebook profile along with mobile phone numbers ending in 02, 42, and 55.

Searches of international investigative databases confirmed that this email address is linked to accounts on Pinterest, Wondershare, Disqus, Nine AU, Instagram and PayPal. The PayPal account has an associated partial mobile phone number of +614***3242, which does not match the Suspect's mobile phone number of 0474 885 042.

It was not confirmed that this profile is being operated by the Suspect.

Randy Gallagher

www.facebook.com/randy.gallagher.100

Technical investigations confirmed that this profile is linked to a partially revealed email address of n*****d@gmail.com.

The profile does not contain a profile picture or cover picture and does not display any public posts. The profile has four friends, including Steve P May, who is noted to be Facebook friends with Ike Rush.

https://www.facebook.com/stevenphillipmay/

Other friends include Kerin Thorne, Maarja Maasik, and Lance Kerslake.

Further analysis of this profile was conducted, where no additional content was identified.

Searches of consumer and investigative databases did not identify any individuals in the name Randy Gallagher with an email address matching the format n*****d@gmail.com.

No evidence was identified to confirm this profile as linked to the Suspect.

Don't Meet Me (Sydney Sex Pests)

www.facebook.com/groups/364032873189154

The About section of the group states:

> *"A community for sharing information and experiences about individuals or profiles on Grindr, Scruff, and similar platforms that you might want to steer clear of.*
>
> ***Public***
> *Anyone can see who's in the group and what they post.*
> ***Visible***
> *Anyone can find this group."*

A Facebook profile in the name Ike Rush is listed as the group's Admin and as having created the group on 22 February 2024. (*See appendix*)

The group has 16 members, the most recent of whom, Eliot Hastie, joined three months prior to the investigation.

Analysis of this page identified 15 posts containing text message exchanges and shared pictures in the context of hook-ups and misaligned expectations.

Targeted searches of this page did not identify any information regarding the Client.

Subject Instagram Accounts

The Client identified eleven Instagram accounts as relevant to the investigation, two of which were considered by the Client as more salient to than the rest, being @beat_slaya and @bjow_ett.

@beat_slaya

www.instagram.com/beat_slaya

Technical investigations confirmed that this account is linked to a partially revealed email address of i**********1@gmail.com, which is noted to align with the format of the email address ike.rushton21@gmail.com.

Searches of international investigative databases confirmed that the email address of ike.rushton21@gmail.com is linked to an Instagram account.

Analysis of this account identified that its profile picture matches that of the Suspect's Facebook profile in the name of Ike Rush. The account's bio states:

> *"Ike Rush*
> *@beat_slaya*
> *Me"*

The account is private and was created in May 2022. It has published eight posts, has 100 followers, and is following 180 accounts.

Although not confirmed, it was considered likely that this account is operated by the Suspect.

@bjow_ett

www.instagram.com/bjow_ett

Technical investigations confirmed that this account is linked to a partially revealed email address of i**********1@gmail.com, which is noted to align with the format of the email address ike.rushton21@gmail.com.

The account was created in February 2023 and has not published any content. It does not have a profile picture, has one follower, and is following three other accounts, @curtis_beck369, @enrolai_org, and @hellueeee. Checks of these accounts did not identify any connections to the Suspect.

It was not confirmed that this account is operated by the Suspect.

@bren_jowett

https://www.instagram.com/bren_jowett

Technical investigations confirmed that this profile is linked to a partially revealed email address of l*******t@gmail.com.

The bio states:

> *"Bren Jowett*
> *Regularly pleasant"*

Analysis of this profile identified that it has a profile picture of a cat, has 64 followers and follows 78 accounts. It is set to private and has not published any posts. The date that the account was established was February 2023.

This account was not confirmed as being linked to the Suspect.

@ant.hadjakis

www.instagram.com/ant.hadjakis

Technical investigations confirmed that this account is linked to a partially revealed email address of a**********@gmail.com.

The account was created in April 2024, has 14 followers, and follows 39 other accounts. No content has been published to the account. The profile picture is the same image of a crown used by the Facebook profile in the name Anthony Hadjakis.

It was not confirmed that this account is linked to the Suspect.

HumphreyDinkum

www.instagram.com/humphreydinkum

Technical investigations confirmed that this profile is linked to a partially revealed email address of a**********@gmail.com.

This profile has no profile picture, has not published any posts, has no followers' and is not following any other accounts. The account was established in July 2024.

It was not confirmed that this account is linked to the Suspect.

@aaron.gallagher.90410

www.instagram.com/aaron.gallagher.90410

Technical investigations confirmed that this profile is linked to a partially revealed email address of a*g@g**.com.

This account was created in April 2020 and the profile picture is a selfie of a man wearing a hat. The only post contained on the account was published on 20 April 2020, is the same picture and is tagged with a location of Sydney, Australia. This picture has been liked by 29 other accounts, none of which seemed to obviously link to any other pieces of evidence. The post's only comment, by @kaarin_maasik, was of interest, however.

"Miss you  *"*

It is noted that a Maarja Maasik is a Facebook friend of the Subject Facebook profile in the name Randy Gallagher.

https://www.instagram.com/maarjamaasik/

Technical investigations confirmed that this profile is linked to the partially revealed email addresses of m*********@gmail.com and m*****2@h**.ee, as well as a mobile phone number ending in 08.

Analysis of this Instagram's accounts followers determined that two of the Subject accounts are following her, however she is not following them back.

It was not confirmed that the Aaron Gallagher account is linked to the Suspect, and may be the legitimate profile of the individual listed as a co-defendant in a previous court case with the Suspect.

Pottspointcentralhotel

www.instagram.com/pottspointcentralhotel

(*See appendix*)

Technical investigations confirmed that this profile is linked to a mobile phone number ending in 42, which aligns with the Suspect's mobile phone number as provided by the Client.

This account was created in October 2021 and its profile picture is of a fine polka dot pattern. The account had not published any posts, was followed by 16 accounts, and followed four other accounts. This account is following @tenant.defenders and is being followed by the account @rentersaustralia.

It is noted that the Suspect left a one-star review for the Potts Point Central Hotel using the Google account linked to his email address of ike.rushton22@gmail.com.

Open source searches identified that the hotel's official Instagram profile is no longer valid. (*See appendix*)

Given this negative review and the partial mobile phone number linked to the account aligning with the Suspect's, it is considered a strong possibility that the Suspect is impersonating the hotel via this account.

@rentersaustralia

www.instagram.com/rentersaustralia

Technical investigations confirmed that this account is linked to a partially revealed email address of i*e@t**********.au, aligning with the Suspect's email address ike@tenantdefence.com.au. Further technical investigations identified that it is linked to a mobile phone number ending in 42 which aligns with the last two digits of the mobile phone number provided for the Suspect.

The account was created in April 2021 and contains a profile picture of a logo of three houses intertwined. The account had published three posts, was followed by 61 accounts, and is following 56 other accounts. The posts appear to be advocating for renters' rights and contain links to the Renters Australia's website, which was not active at the time of the investigation.

Given the partial email address and mobile phone number linked to this account, it was considered likely to be controlled by the Suspect.

@td.56455

www.instagram.com/td.56455

Technical investigations confirmed that this profile is linked to a partially revealed email address of a*****9@**.com.

The account was created in January 2022, had one former username, and contained a profile picture matching that on the Karen Thorne Facebook profile. Although the account is locked, it was identified that no posts had been published, it has no followers, and follows one other account. The display name is the word "Nah".

It was not confirmed that this account is linked to the Suspect.

@karen.thorne.3762

www.instagram.com/karen.thorne.3762

Technical investigations confirmed that this profile is linked to the partially revealed email addresses of t**********4@gmail.com and k*********0@gmail.com, as well as a mobile phone number ending in 76.

The display name is listed as Kerin Thorne and the account was created in September 2020. The profile picture is a painting of a ginger-haired girl asleep and cuddling a ginger cat. The account has not published any posts, has seven followers, and is following 62 other accounts.

It is noted that the accounts @beat_slaya and @rentersaustralia are following this account and that this account is following various accounts related to tenancy matters including:

@ratetherental_australia
@rentersaustralia
@tenantresourcecenter
@tenantsnsw
@better_renting

It was not confirmed that this account is linked to the Suspect and it is likely linked to a friend or acquaintance of the Suspect.

@gallagherrandy88

www.instagram.com/gallagherrandy88

Technical investigations confirmed that this profile is linked to a partially revealed mobile phone number of +234 *** *** **97 and a partially revealed email address of o**********7@gmail.com. It is noted that +234 is the international calling code for Nigeria.

The account was created in January 2020, is private, and contains a display name of Randy Gallagher. It has had one former username and contains a profile picture of a tabby cat. The account has published three posts, has two followers, and is following 177 accounts.

Given its link to Nigeria, it was considered unlikely this account is linked to the Suspect.

Other Social Media Accounts

YouTube

A Youtube account was provided by the Client for the Suspect.

https://www.youtube.com/@HumphreyDinkum

Analysis of this account identified that it displayed no content and no information was identified to confirm it as being linked to the Suspect.

TikTok

A TikTok account was provided for the Suspect.

https://www.tiktok.com/@slaya_ike

This account was following 33 other accounts, was followed by 17 accounts, had no likes and no bio. A single TikTok was published by the account, which was a photograph of a man with a cigarette in his mouth and a music track accompanying it. The tags that are linked to this post are: @brodyhull @brodie.hull5 @Brodie hull @Brodie Hull @hullybrodie @user9312907073689 @BŕōdȉēHùĺĺ

Analysis of the links did not identify any information of relevance.

Searches of TikTok using the name Brodie Hull identified an account with the same man as pictured in the @slaya_ike account.

https://www.++.com/@brodiehull

Analysis of this account identified numerous videos of a man miming to music and recording himself with different filters.

The Client provided a text message exchange with an individual he believed was named Brodie Hull.

The exchange reads:

> Client: "*Hey Brodie. There is a guy stalking you online. This guy is stalking me as well. He posted this on tik toc and it's you. Let me know if you want to compare notes about him.*"
>
> Brodie: "*Weird yeah ive been dealing with id theft issues and someone pretending to be me. "*

(See appendix)

Given the strong likelihood that the Suspect operates numerous accounts that include the names Slaya and Ike, along with the above exchange between the Client and an individual he believed was Brodie Hull, it was considered possible that the Suspect also impersonated Mr Hull.

Username Searches

Searches were conducted of international investigative databases for the usernames beat_slaya, slaya_ike, humphreydinkum, tenantdefence, tenancy.disputes, ike_rushton, issacrushton, issac_rushton, zac20, and issac_88, where several results of potential relevance were identified.

The username beat_slaya was identified as being linked to a DubSmash account with an associated email address of fartypantsninja@gmail.com. Technical investigations confirmed that this email address is currently valid and linked to a Google account with ID 110304552135573156941. Analysis of the associated Google account identified this user as being located in India and the email address was considered unlikely to belong to the Suspect.

The username issacrushton was identified as being linked to a Zynga account with an associated email address of izac23@hotmail.com. Technical investigations confirmed that this email address is currently valid and linked to the partially revealed email addresses of iz*****@allerskog-krantz.se and iz*****@outlook.com, along with a mobile phone number ending in 31. The website allerskog-krantz.se was identified as being a Swedish building company, and it was therefore considered unlikely that the email address izac23@hotmail.com is linked to the Suspect.

Summary of Assessment

The Client reported that he has been the target of ongoing online impersonation, harassment and cyberstalking through social media and encrypted messaging platforms beginning around 2021. The majority of this offending activity was reported to have taken place in groups on the Telegram app, as well as on the Instagram, Facebook and LinkedIn platforms.

Two accounts in the names of @frost_rich and @The_real_Tony_smith, both with the display names of Tony Smith, were investigated in terms of their posting behaviours on the Telegram platform.

The @the_real_Tony_smith account was identified as being active in the 'Sydney Party Lads' Telegram channel, and revealed to be advertising the

sale of illicit substances (cocaine, heroin, or methamphetamines) in quantities of points, half grams, grams, 1.75 grams and eight-balls.

The @frost_rich Telegram account was identified as being active in the Sydney Lads Up Late' Telegram channel, and revealed to be advertising the sale of ketamine and cannabis, as well as posting about their purported dark web engagement and potential hacking.

A tracking link was deployed by Cybertrace to the Subject via the @frost_rich account on the Telegram app on 30 April 2025, where an IP address of 103.53.118.254 was obtained. Analysis of the IP address confirmed that it was not linked to a known proxy or VPN. A location of Sydney and an Internet Service Provider (ISP) of Anycast Global Backbone were also identified.

The identity of the individual operating the @frost_rich and @the_real_Tony_smith Telegram accounts was not confirmed.

Anycast technology was understood to be different to regular ISPs in the sense that it is a network addressing and routing method in which incoming requests can be routed to a variety of different locations or "nodes". This means that the same IP address is shared by multiple servers in different locations. Anycast Global Backbone is linked to an operation called Anycast Holdings, which is a subsidiary of the ISP, Swoop.

The Client provided Issac William Rushton as the likely Suspect behind these behaviours. A comprehensive proprietary database, social media, and open source investigation was conducted into Issac, where he was identified as using numerous alias names, and being currently enrolled to vote at Brougham Street, Woolloomooloo NSW 2011. His working history claimed to include a patchwork array of life coaching, insurance brokering, real estate, admin, and web development.

The Suspect had an extensive court attendance history with numerous appearances at the Brisbane Arrests Court between 2015 and 2019, as well as being the protected person in several AVO applications, and having an extensive civil court history as both the plaintiff and defendant, which appears to be primarily related to housing and tenancy issues.

Issac was identified as being linked to the following domains, none of which are linked to currently active websites, through his ABN:

http://evolvealt.org
parkerrushton.com.au
rentersaustralia.com.au
tenancydispute.com.au
tenantdefence.com.au
tenantdefenders.com.au
tenancydisputes.com.au

The following email addresses were identified as being used to register these domains, confirming them as linked to Issac:

ike@aussierenters.com.au
ike@tenantdefence.com.au
ike.rushton22@gmail.com

It is also considered highly likely that the following email addresses associated with Issac's domains are operated by him.

contact@tenantdefence.com.au
ike@tenancydisputes.com.au
ike@rentersaustralia.com.au

In addition, the email addresses ike.rushton@outlook.com and zac20@live.com.au were confirmed as being linked to the Suspect through investigative databases.

Specific investigations of the email address ike.rushton22@gmail.com confirmed it as being linked to a mobile phone number of 0474 885 042, and a Microsoft account using the name Anthony Smith, providing evidence that the Suspect is using the Client's name online.

Analysis of a number of other email addresses, phone numbers, and social media accounts were conducted, where the Suspect was either confirmed or considered highly likely as being linked to the following:

slaya@outlook.com.au
ike.rushton21@gmail.com

www.facebook.com/i.crush.the.competition
www.facebook.com/groups/364032873189154

www.facebook.com/tenantdefenders
www.facebook.com/groups/931393340681530

www.instagram.com/beat_slaya
www.instagram.com/tenant.defenders
www.instagram.com/pottspointcentralhotel
www.instagram.com/rentersaustralia

www.linkedin.com/in/issac-rushton-6740a792/
linkedin.com/in/mark-eldridge-358772223

https://x.com/ike_rushton

https://www.youtube.com/@ikerushton9059

Two further tracking links were deployed to the Suspect via Facebook Messenger, where he was somewhat hostile and extremely cautious, repeatedly querying the engineered pretext. At the time of the close of the investigation, these links had not been engaged with.

This pattern of hostility and mistrust by the Suspect aligned with the same types of communication used by the Subject account @frost_rich.

In terms of intelligence gathered through the course of the investigation, it was considered that the Subject presents with patterns of impersonating people with whom he has had conflict. With likely engagement in the dark web, as a trafficker of illicit substances, fraud and other crimes, such impersonation might serve the dual function of avenging said conflicts, and carrying out illicit activity with impunity. It is therefore vital that law enforcement agencies take action to bring due consequences to bear on the offender, so that he ceases this behaviour.

Recommendations

It is recommended that a request is made of the Telegram application for records pertaining to accounts in the name of @the_real_Tony_smith and @frost_rich.

It is further recommended that a Forensic Data Request be made of Swoop and Anycast Holdings with regard to Anycast Global Backbone and for information pertaining to the specific user of IP address 103.53.118.254 at

11.04 AM (AEST) in Sydney on 30 April 2025. Given that multiple users can be linked to this IP address at a given point in time, it is crucial that browser histories, network traffic and system logs are analysed to determine which websites have been accessed with this IP address at this time and what was posted on them. It is particularly critical that authorities investigate the matter of the user linked to this IP address who has used Telegram to promote the sale of narcotics using the name of the Client.

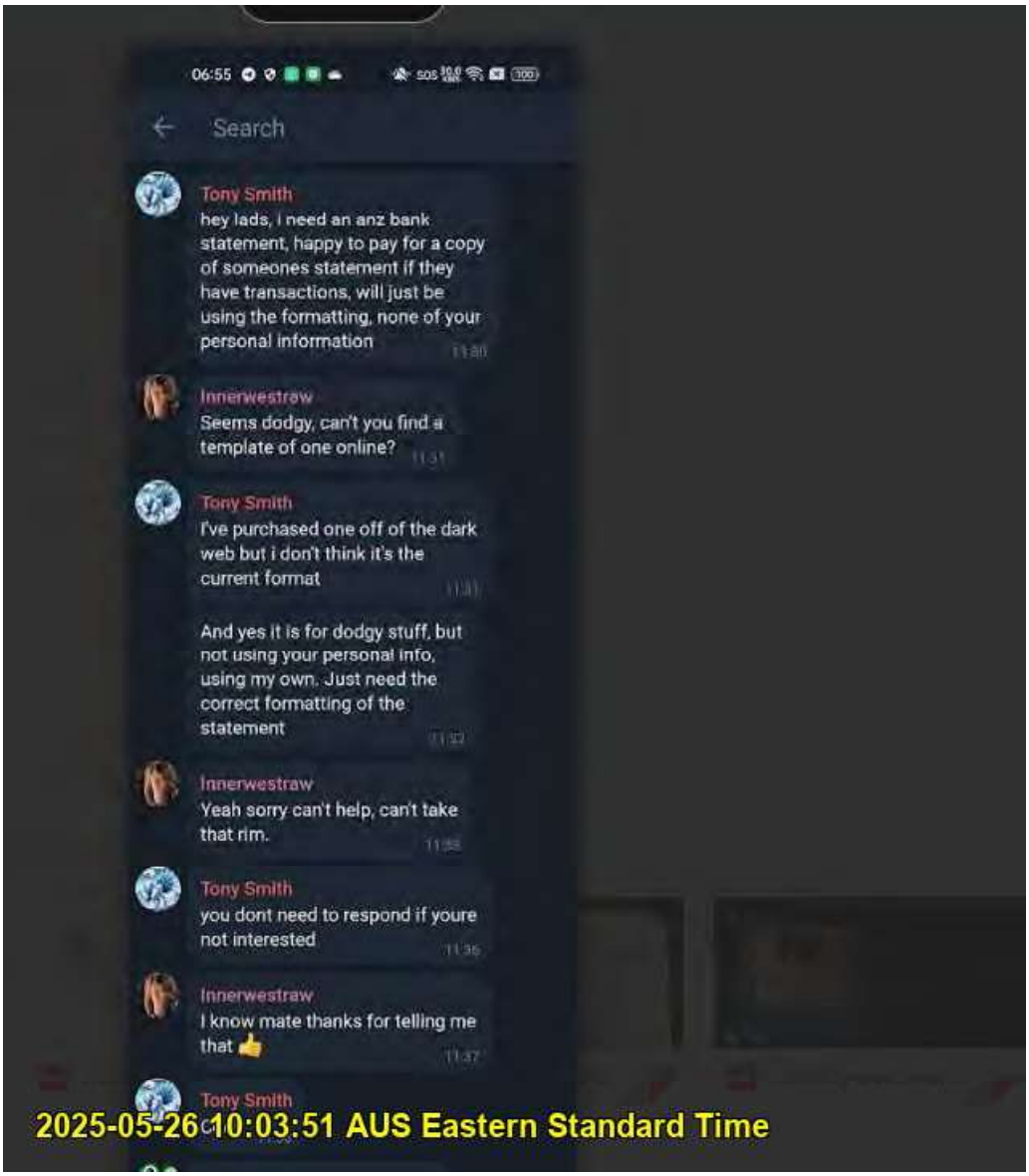
Anycast Global Backbone:	5/15 Phoenix Street, Warragul VIC 3820
Anycast Holdings Pty Ltd:	Level 21, 135 King Street, Sydney NSW 2000 +61 3 5622 4600 noc@anycast.com.au
Swoop Broadband:	1a/ 155 Queen Street, Warragul VIC 3820 1300 665 575 support@swoop.com.au

If you have any further questions in relation to this matter, please contact our office on +61 9188 7896.

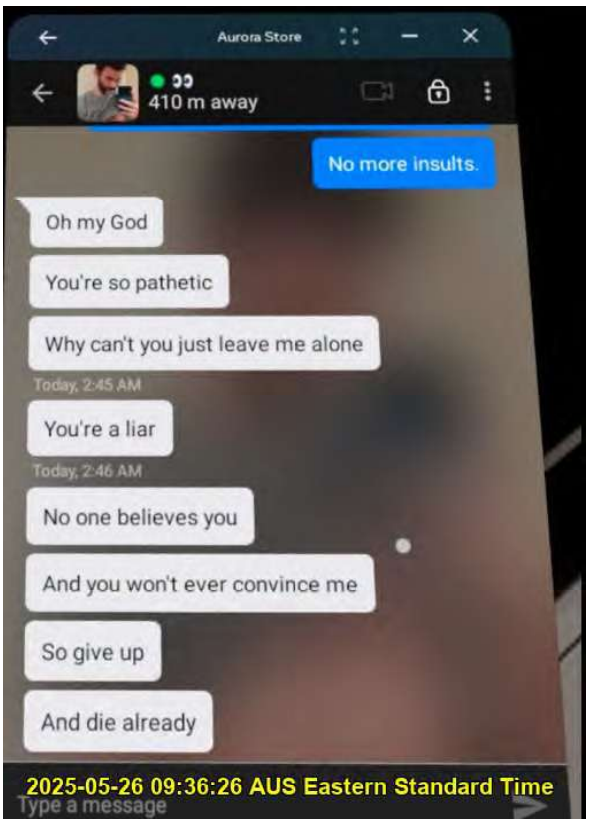
Kind regards,

Dan Halpin
CEO
Cybertrace
www.cybertrace.com.au
E: contact@cybertrace.com.au
Ph. Australia: 1300 669 711
Ph. International: +61 2 9188 7896

Appendices



Comment: A Telegram account in the name of Tony Smith requests an ANZ bank statement.
Source: Provided by the Client

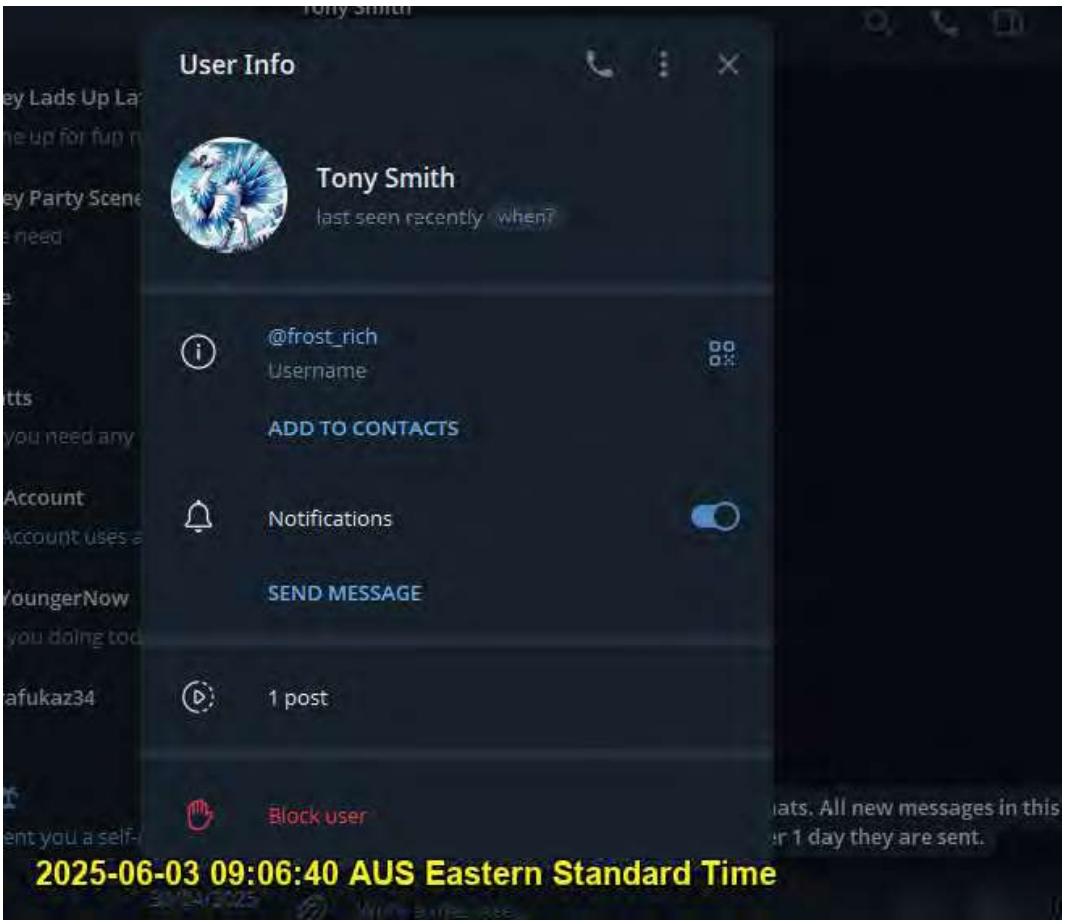


Comment: An exchange between the Subject and the Client.
Source: Provided by the Client

Comment: A Telegram account created in the name of the Client.
Source: Provided by the Client

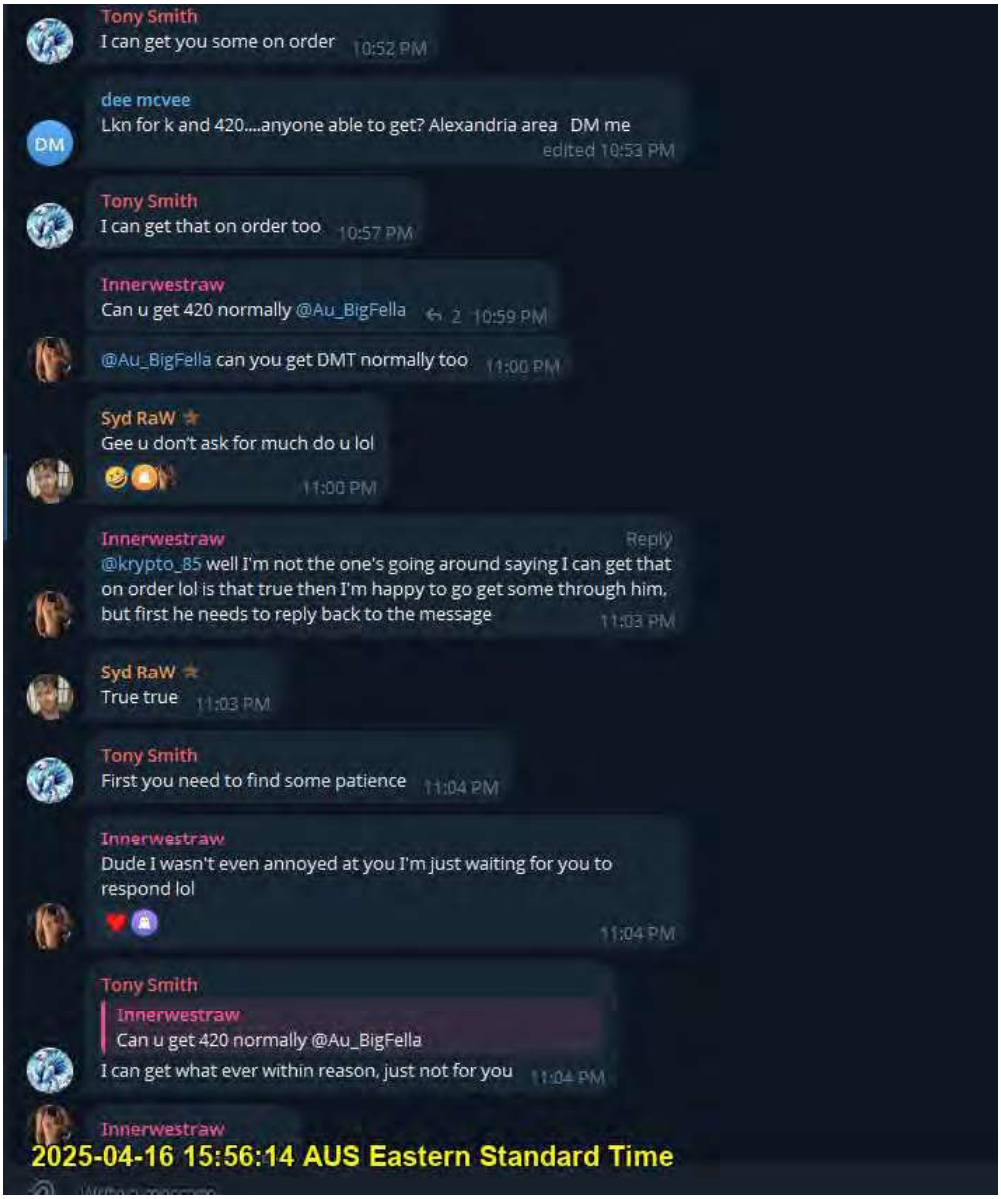
Comment: An account in the name of Tony Smith is in the Sydney Party Lads Telegram channel selling drugs.
Source: Sydney Party Lads Telegram

Comment: An account in the name of Tony Smith is in the Sydney Party Lads Telegram channel.
Source: Sydney Party Lads Telegram



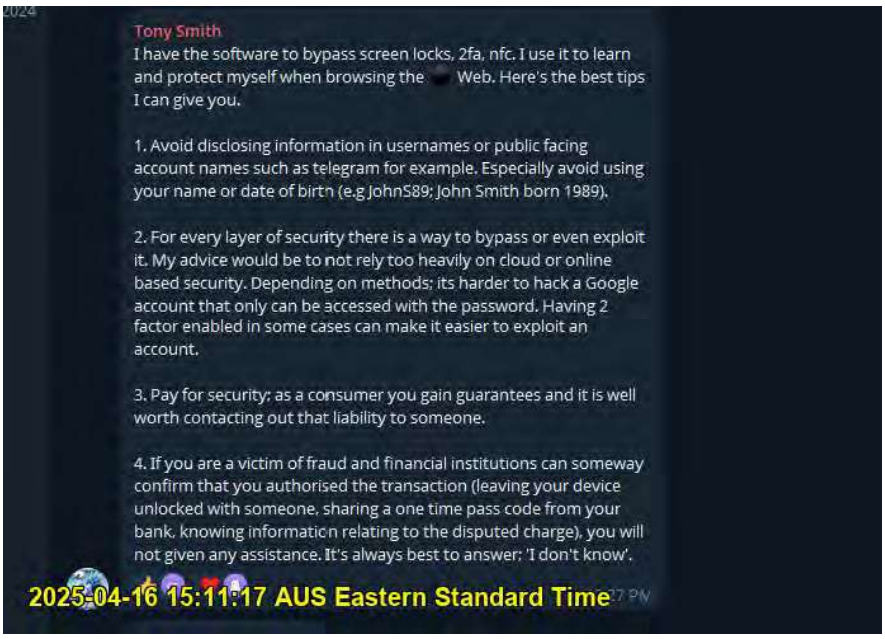
Comment: Subject Telegram account @frost_rich Tony Smith.
Source: Telegram

Comment: Channel bio
Source: Telegram Sydney Lads Up Late Telegram



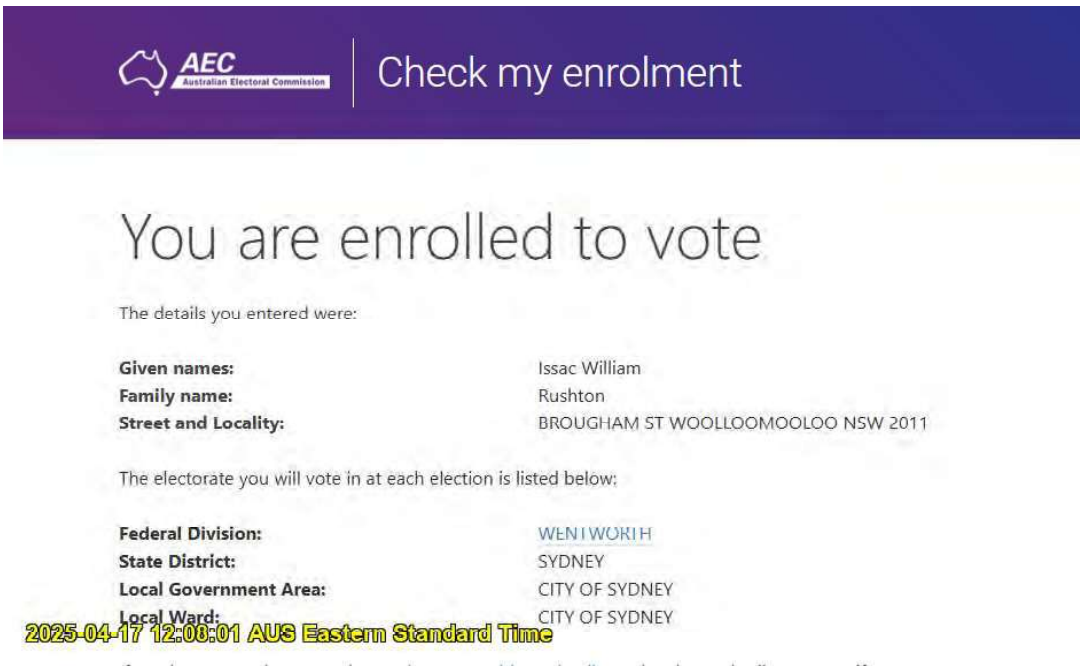
Comment: An account in the name of Tony Smith referring to being able to get cannabis, DMT, and ketamine.

Source: Sydney Lads Up Late Telegram channel



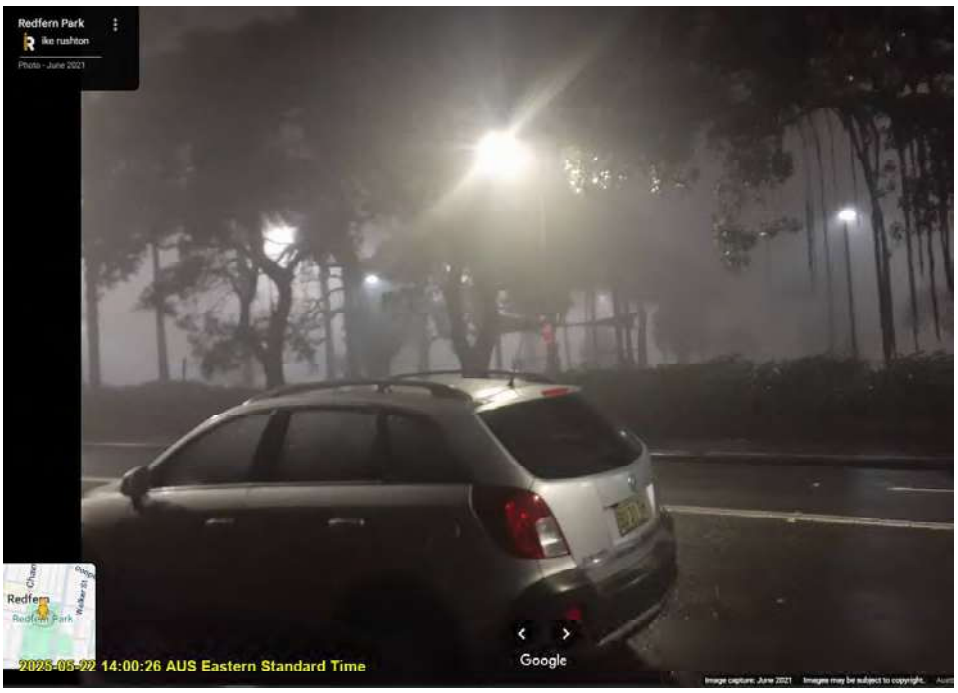
Comment: An account in the name of Tony Smith giving cyber security advice and advising the use of one's real name.
Source: Sydney Lads Up Late Telegram channel

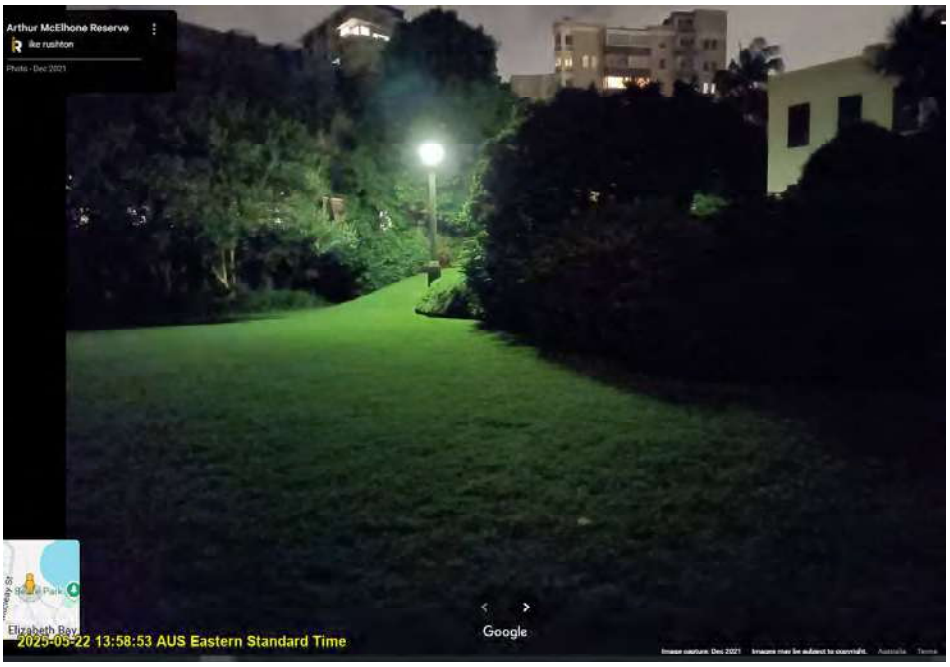
Comment: Syd Raw runs Sydney Party Lads Telegram channel. Tony Smith profile invited him to join Sydney Party Animals.
Source: Sydney Party Lads Telegram



Comment: The Suspect is enrolled to vote at Brougham Street Wooloomooloo NSW 2011.
Source: AEC

Comment: Confirmation the Google account ike.rushton22@gmail.com is linked to the mobile phone number 0474 885 042.
Source: Google





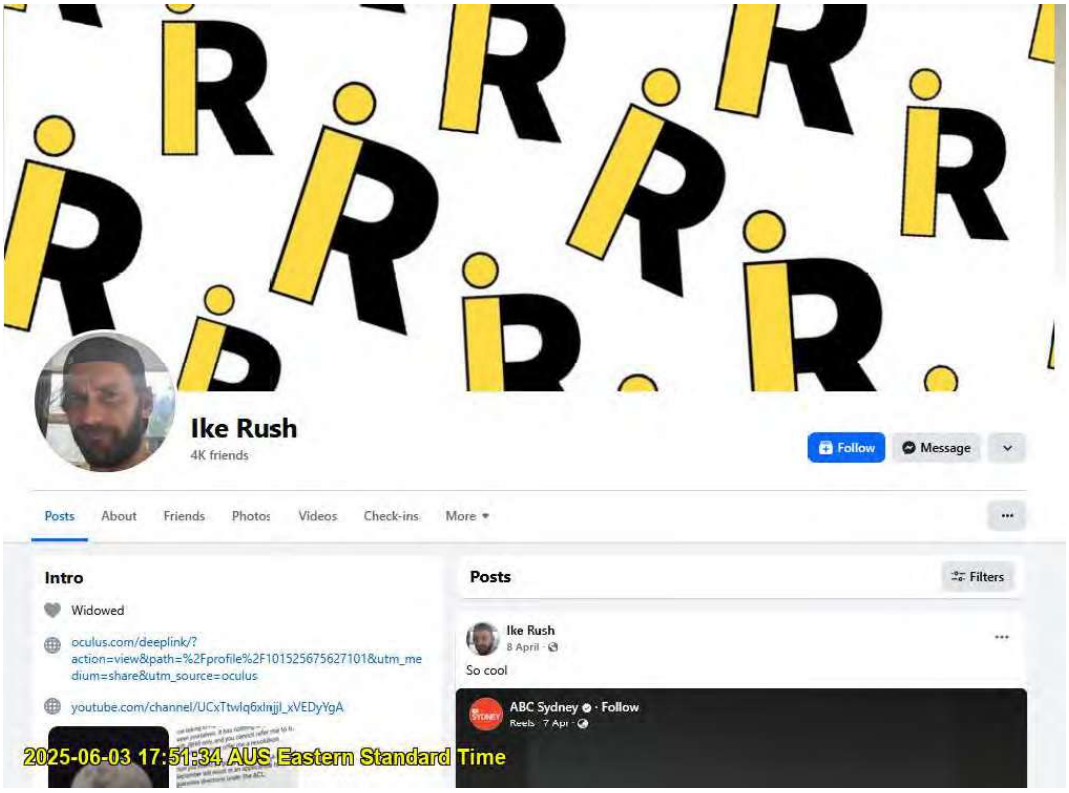
Comment: Google account linked to ike.rushton@outlook.com displays pictures of a park, with an apartment block in view and car with visible licence plates.

Source:

https://www.google.com/maps/contrib/109750812710196980061/photos/@-33.8698266,151.2268359,3a,75y,90t/data=!3m7!1e2!3m5!1sCIHM0ogKEICAgIDG2-Te8QE!2e10!6shttps:%2F%2Flh3.googleusercontent.com%2Fgps-cs%2FAIky0YVWdb-Y8j62lbtZlsYJHZzXejs1dAgF7X8SxQHVkzRs9pqAAmuLhPdNpiWEUrTFrMy6cfCYMQQAkokLt61jJR8-oY3WeTdcJQElLgeicfdceq1iu2GvACEkzzbr2gXlF80E1JlD4A%3Dw365-h273-k-no!7i4000!8i3000!4m3!8m2!3m1!1e1?entry=ttu&g_ep=EgoyMDI1MDUxNS4xIKXMDSoASAFQAw%3D%3D

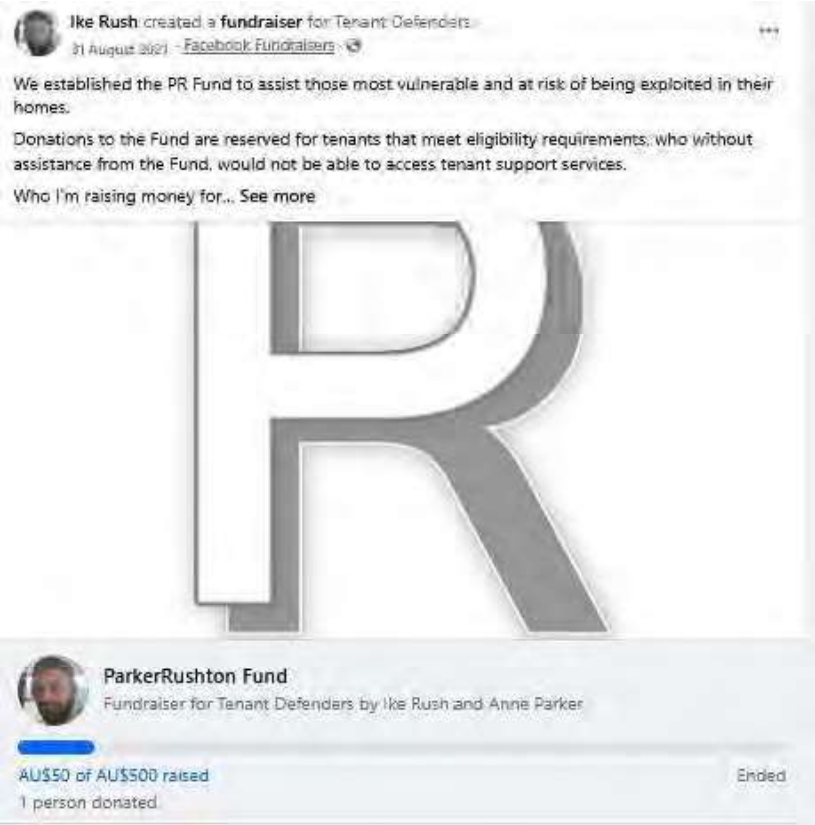
Comment: The profile picture for the Dropbox account linked to ike.rushton22@gmail.com

Source: https://dl-web.dropbox.com/account_photo/get/pid_uphoto%3AAAAAAHb7gnzhFDw2HQRbfZO1DbzHIqoKy1tUjV7EIgCudeoocw0fCMw_dvSIqdTEKrGwaGfkdBzgiGIBcmsg?size=128x128&vers=1628633885774

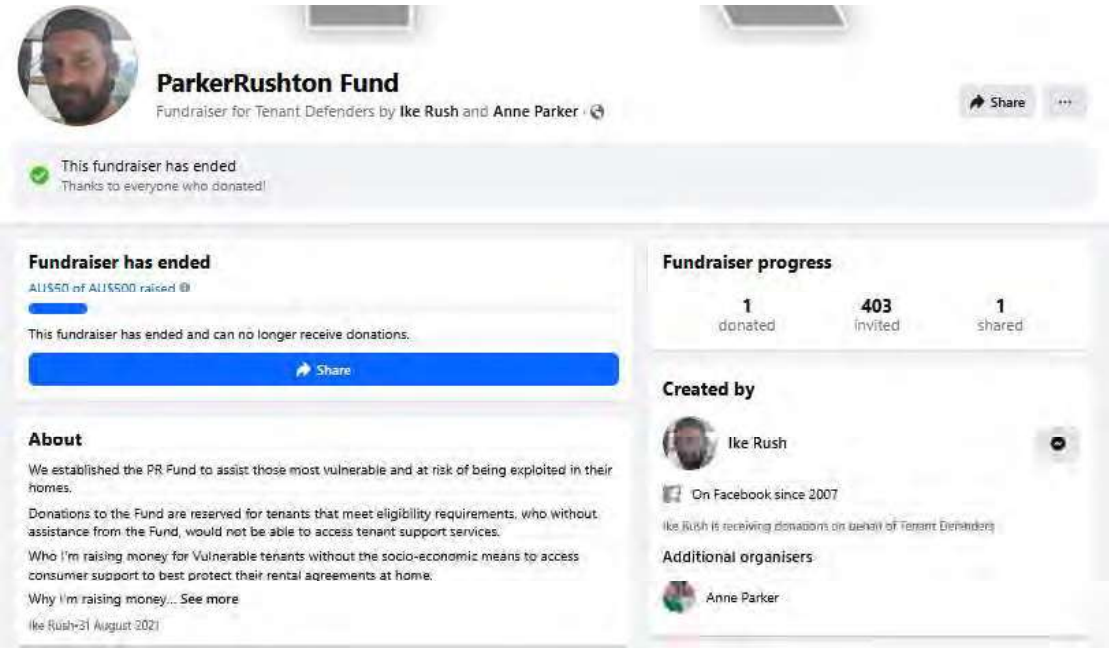


Comment: Facebook profile in the name Ike Rush.

Source: https://www.facebook.com/i.crush.the.competition



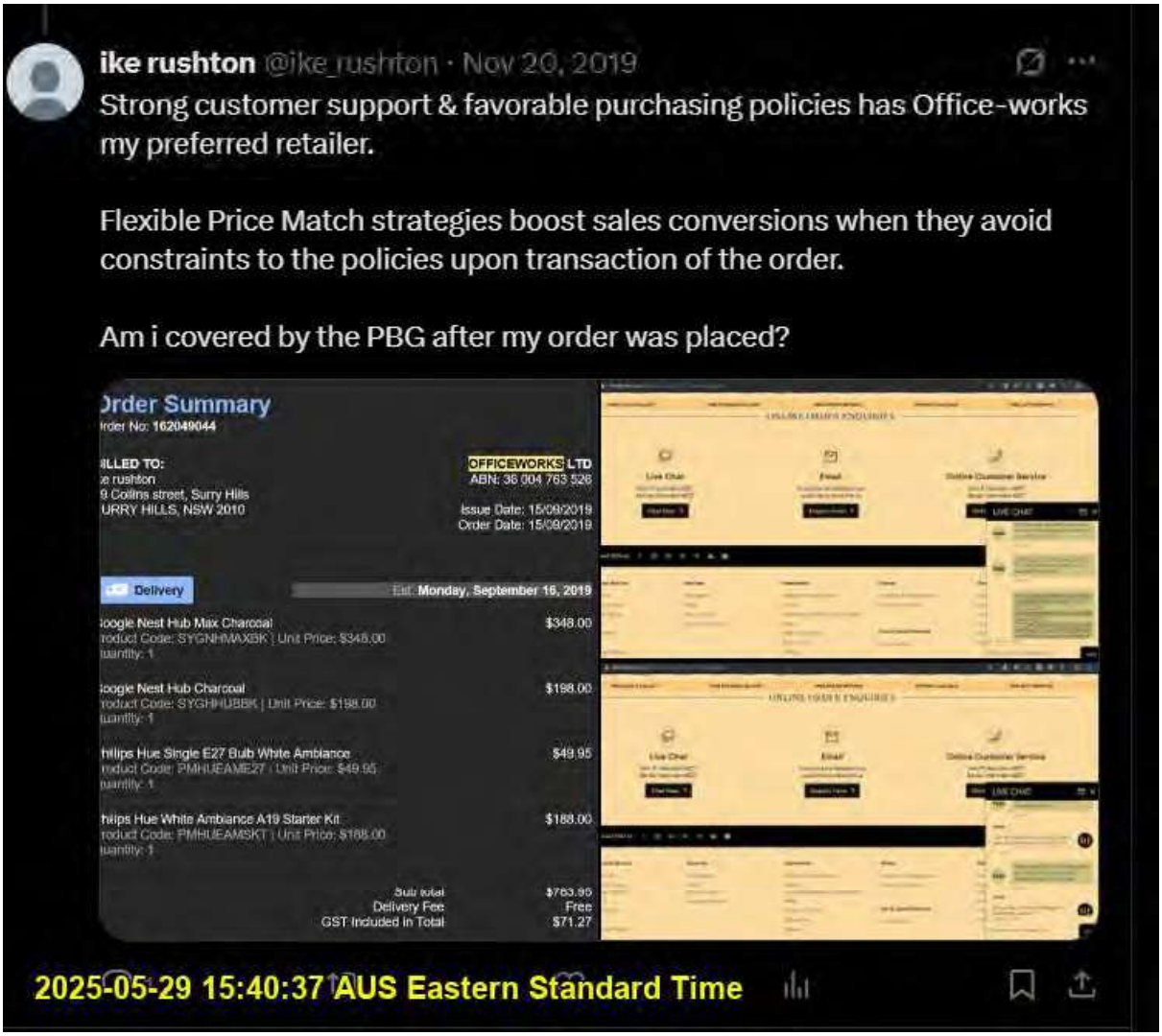
Comment: Fundraiser for Tenant Defenders published on the Facebook profile Ike Rush (@i.crush.the.competition).
Source: https://www.facebook.com/share/16JxQK4dLN/



Comment: Fundraising page showing the Ike Rush profile as having been created in 2007.
Source:
https://www.facebook.com/donate/3764212447011830/3764215080344900/

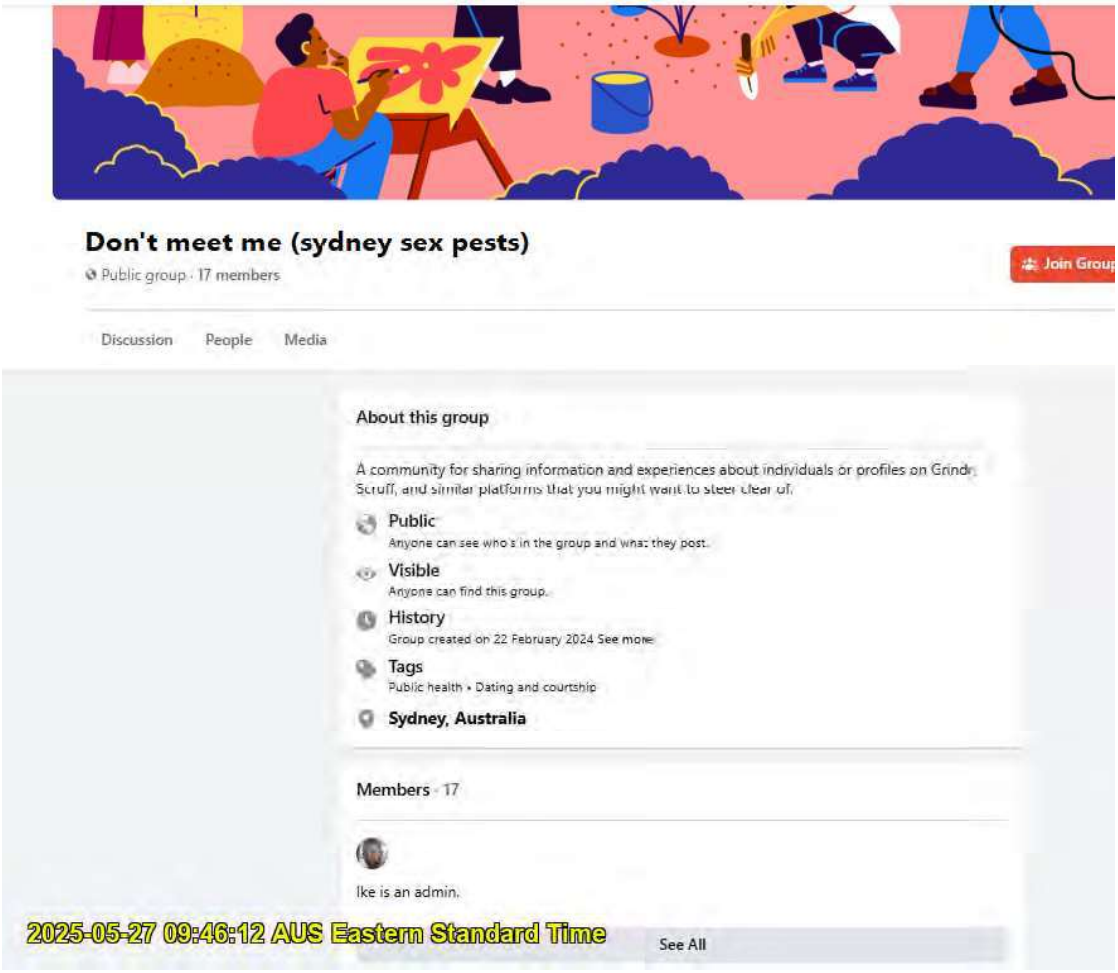
Comment: Issac (Ike) R. LinkedIn profile.
Source: https://www.linkedin.com/in/issac-rushton/

Comment: Issac Rushton profile on LinkedIn
Source: https://www.linkedin.com/in/issac-rushton-6740a792/

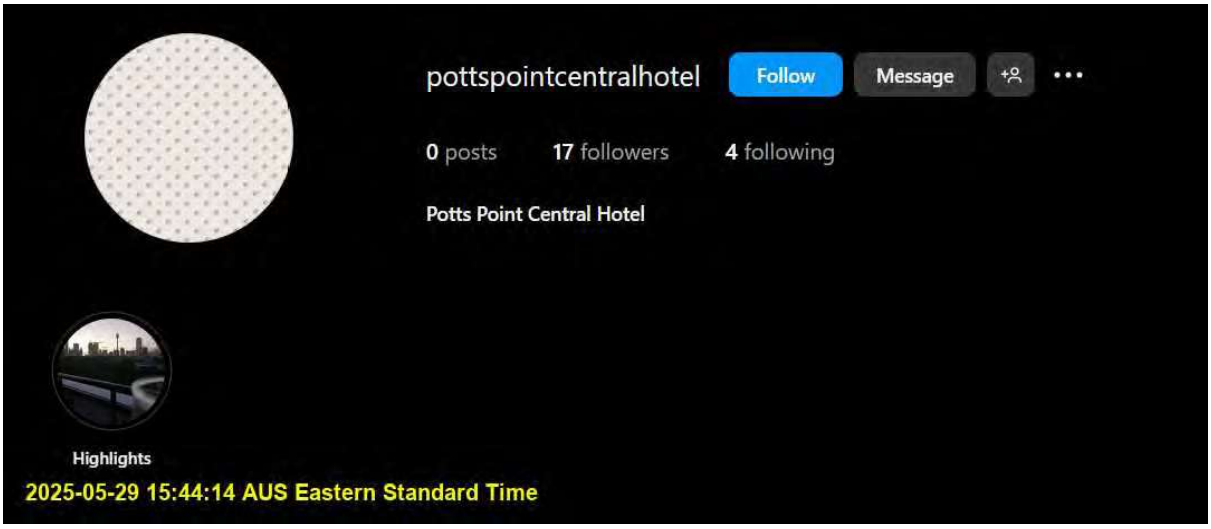


Comment: An X account in the name of the Suspect appealing to Officeworks' pricematching policy.
Source: https://x.com/ike_rushton/with_replies

Comment: Karen Thorne's most recent profile picture
Source: https://www.facebook.com/share/1ah16cNzae/

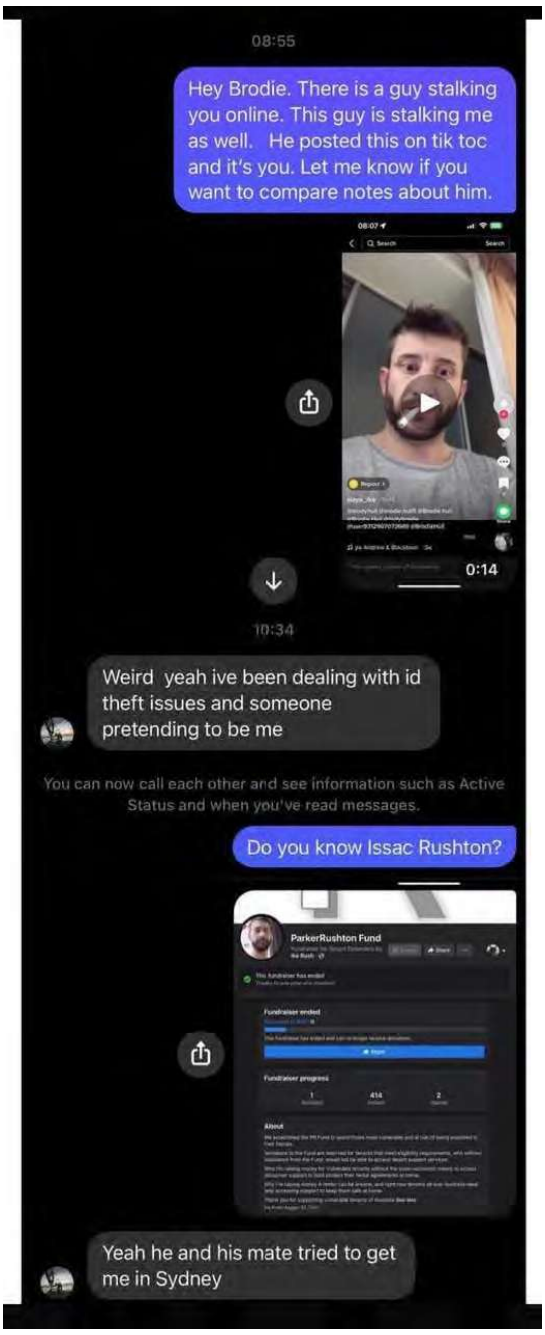


Comment: Ike Rush is listed as the Admin of the Don't meet me (sydney sex pests) Facebook group
Source: www.facebook.com/groups/364032873189154



Comment: Pottspointcentralhotel Instagram account.
Source: https://www.instagram.com/pottspointcentralhotel/

Comment: The official Instagram account for Sydney Potts Point Central Hotel is not valid.
Source: https://www.instagram.com/pottspointcentral/



Comment: An exchange between the Client and an individual in the name of Brodie Hull.
Source: Provided by the Client

JUSTICE DENIED

A five-year case of identity theft, police inaction, and one man's fight for the truth.

5+

Years of Inaction

Reports of serious crimes were repeatedly filed starting in 2019, with formal complaints since 2021.

1

Independent Report

A forensically sound report providing irrefutable evidence was commissioned and subsequently ignored by police.

1

Actionable IP Address

The perpetrator's IP address was captured, traced, and presented to police, who failed to act on the lead.

A Timeline of Dismissal

2019 - 2021: The Beginning

The victim, Tony Smith, begins reporting a campaign of cyberstalking, harassment, and impersonation by Issac Rushton. Despite numerous reports to Crime Stoppers and local police, his concerns are dismissed.

2022: Malicious Prosecution

Mr. Smith is arrested on a false bail breach charge based on a phone number later proven impossible by the telecommunications provider. This marks a turning point where the victim is treated as the perpetrator.

2023: Evidence Ignored

Attempts to provide verifiable digital evidence to clear his name are consistently refused or confiscated by police. Senior officers dismiss criminal complaints as "civil matters."

2024: Communication Banned

After persistent attempts to seek justice, Kings Cross Police impose a communication ban, effectively silencing the victim. Key officers spread false information, leading to the loss of his job and home.

June 3, 2025: Irrefutable Proof

A privately commissioned report by Cybertrace Pty Ltd provides conclusive forensic evidence linking Mr. Rushton to the crimes. The report and its recommendations are presented to police, who take no action.

Evidence Provided vs. Police Response

☑ Evidence Submitted by Victim

Crime Reports: Numerous reports on drug dealing & impersonation.

Digital Records: Telstra/Optus data disproving police claims.

Confiscated Phone: Contained evidence of perpetrator's abuse.

Subpoena Request: Asked for Meta/Instagram data to verify facts.

Forensic Report: Full Cybertrace report with IP address and alias links.

✖ Response from NSW Police

Dismissal: Labeled as "civil disputes" or "not in public interest."

Refusal: Ignored verifiable telco records.

Inaction: Failed to use or return evidence on confiscated phone.

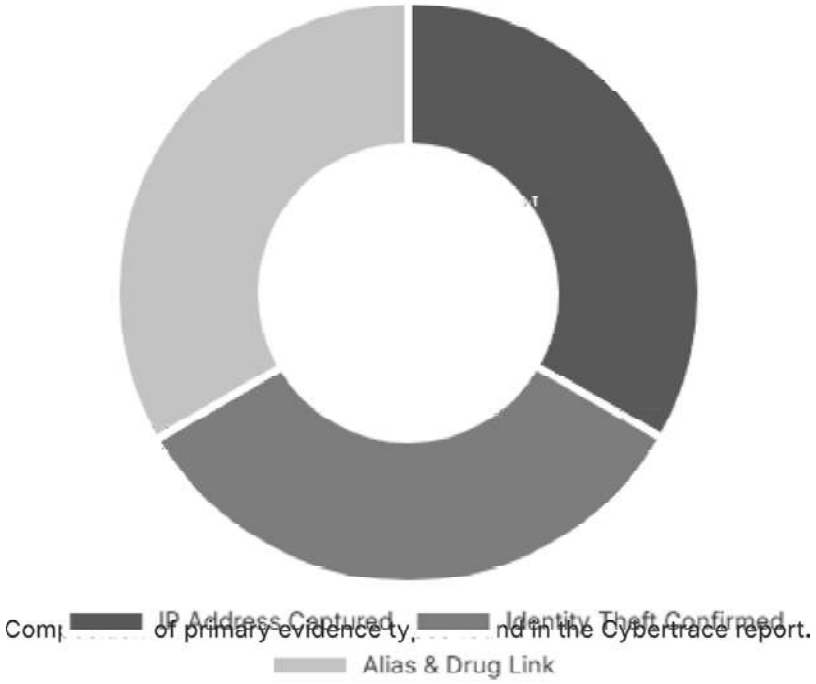
Denial: Refused to subpoena independent records from Meta.

Neglect: Took no action on the Cybertrace report's actionable leads.

The Independent Investigation

Frustrated by police inaction, a private forensic investigation was commissioned from Cybertrace Pty Ltd. The report provided clear, actionable evidence that was ignored.

Key Findings of the Report



Comp of primary evidence ty, nd in the Cybertrace report.

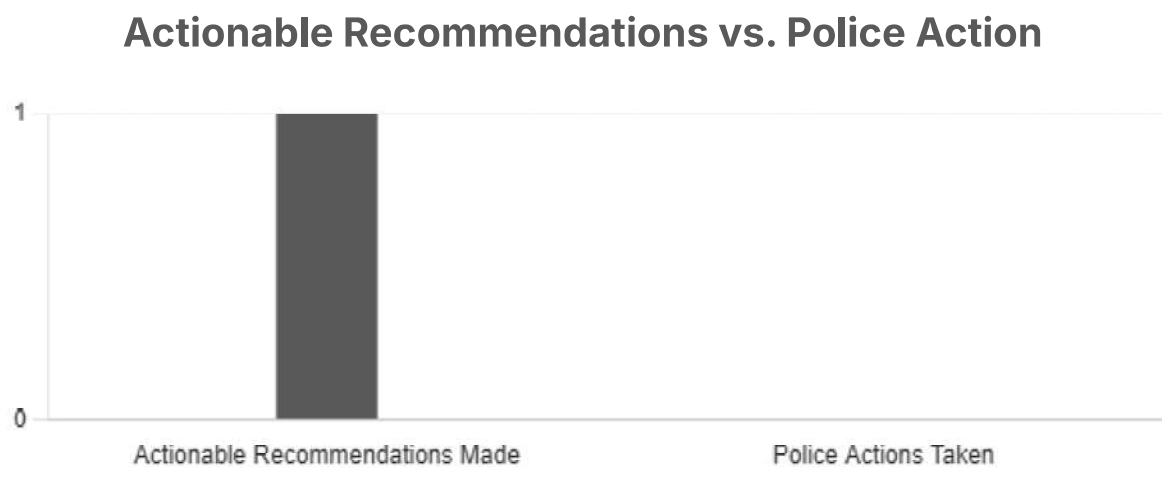
CONFIRMED IDENTITY THEFT

A Microsoft account linked to the perpetrator's email (`ike.rushton22@gmail.com`) was created using the victim's name, "Anthony Smith."

CAPTURED IP ADDRESS

103.53.118.254

Traced to Swoop/Anycast in Sydney on April 30, 2025. Financial records link the perpetrator to the ISP.



Comparison of formal recommendations made by Cybertrace versus actions taken by NSW Police.

A Call for Accountability

The complaint filed with the NSW Ombudsman seeks to resolve years of injustice. The path forward requires three fundamental actions.

1

Full Independent Investigation

↓

2

Directive for Police to Act

↓

3

Acknowledgement of Failure

Take Action

Use these AI-powered tools to help demand justice and raise public awareness. Click a button to generate content based on the case file.

✨ Generate Draft Email to an MP

✨ Suggest Questions for Officials

✨ Create Social Media Post

This infographic summarizes the complaint submitted to the NSW Ombudsman based on documented evidence. The subject seeks to bring public awareness to systemic failures in addressing cybercrime and protecting victims.

The Hon Yasmin Catley MP
Minister for Police and Counter-terrorism
Minister for the Hunter

Ref: MINS-522608304-20911
F/2025/43622

The Hon Tanya Plibersek MP
Minister for Social Services
Federal Member for Sydney
PO Box 2676
STRAWBERRY HILLS NSW 2012

Tanya.Plibersek.MP@aph.gov.au

Dear Minister,

Thank you for your correspondence on behalf of Mr Anthony Smith regarding allegations of identity theft and misconduct by police.

The NSW Government and the NSW Police Force (NSWPF) take all complaints regarding policing very seriously. Complaints against employees of the NSWPF are managed in accordance with Part 8A of the *Police Act 1990*. Independent oversight of this process is exercised by the Law Enforcement Conduct Commission.

I am advised that the allegations raised by Mr Smith have been fully investigated by the NSWPF's Kings Cross Police Area Command (PAC) on a number of occasions. Police have also engaged with Mr Smith over a period of time in relation to his concerns and he has been informed that there is insufficient evidence to substantiate claims of identity theft.

I am further advised that on 8 July 2025, an officer from Kings Cross PAC spoke with Mr Smith to further discuss his concerns, where he was provided with additional information on the outcome of the investigation by police.

Should Mr Smith have further concerns, please encourage him to contact Kings Cross PAC on (02) 8356 0099.

Thank you for writing about this matter.

Sincerely,

Yasmin Catley MP
Minister for Police and Counter-terrorism
Minister for the Hunter

52 Martin Place Sydney NSW 2000
GPO Box 5341 Sydney NSW 2001
02 7225 6100
nsw.gov.au/ministercatley

🔥 TT +10

27 July 2024

12:46

Tony Smith

From now until around 8pm I have a registered nurse available to admin for anyone in Kings Cross.

$50 per admin, or if you make a purchase it's free.

👍 1

1 12:48

$₹

Tony

From now until around 8pm I ha...

14:18

I'm Scott

I was thinking he was a cop

I just got out of jail

He said you were jail

That's me I'm Scott. Issac is a piece of shit and gave me up

Yeah he is hey

What did you done for

Doing a jewellery store over

Did issac have anything to do with it?

That's issac drug store

Yeah he's a bad junkie dog

Why do the police protect him

Because he's an informant

Stalker account

He lies and makes false accusations against. I've got more charges coming

Because of the new charges I'm not adding people to the account at the moment. So many of the follow requests are liar's stalker accounts and police accounts as well.

Everyone knows he's liar he does it to everyone

Lies to get people charged?

While he runs a drug shop

Hes doing illegal shit all the time. But thinks he is above the law.

Yes. Fuck you. And he is

The police know he lies to them. And they keep charging me. It's fucked me. He so abusive

He is abusive I used to be his friend until he stole all my stuff then dobbed me into the cops

I have been telling the police about the drug dealing. To try and stop him from ruining me with false accusations. And they do nothing. Scott he's a psychopath... He's really dangerous

I'm trying to make public what he does and what the police are letting him do

Yeah I know he claims he was raped and it's all just lies he just didn't like it because he was just trying to get drugs for free

Raped by who?

You apparently

That's fucked. He tried to set me on

The whole gay screwe knows he's a heino dog and a drug scab

I got a cool video of it I think you

Yeah he's a piece of shit

His whole family are drug addict losers

I think he does this scam Crypto scam, where he steals people's crypto wallets. I see him doing stuff on.

How aged he got fast

The police have ruined me. And they

I'm sorry to hear he screwed you over as well. The police have a lot to answer for

Fuck mate you didn't deserve any of that

Ek he's out of control

He's crazy

NSW Police Force

21 February 2025

D/2025/201535

Mr Tony Smith
als1969@icloud.com

Dear Mr Smith,

Thank you for your recent correspondence, dated 11 February 2025. We have reviewed the concerns you raised, and, after careful consideration, we have decided that we will not be addressing any further correspondence from you on this matter.

Please be advised that should you require assistance in the future, in the event of an emergency, you are encouraged to immediately call Triple Zero (000) for urgent situations.

Yours sincerley,

David El-Badawi
D/A/Superintendent
Commander

Kings Cross Police Area Command
1-15 Elizabeth Bay Road, Elizabeth Bay NSW 2011
T 02 8356 0099 **F** 02 8356 0019 **W** www.police.nsw.gov.au
TTY 02 9211 3776 for the hearing and speech impaired ABN 43 408 613 180

Ian Steptoe

From: #NO-REPLYMES
Sent: Tuesday, 2 September 2025 08:09
To: tanya.plibersek.mp@aph.gov.au
Subject: Reply to correspondence F 2025 43622 . [SEC=OFFICIAL]
Attachments: Ministerial response - Plibersek MP obo Smith F 2025 43622.pdf

This email address is not monitored for replies.

Please find attached a response to your correspondence.

To respond to the Office of the Minister for Police and Counter-terrorism and Minister for the Hunter online, please visit**:** **https://www.nsw.gov.au/nsw-government/ministers/minister-for-police-and-counter-terrorism**

To respond to the NSW Police Force online visit**:** https://www.police.nsw.gov.au/contact_us.

Regards

NSW Police Force.

NSW Police Force
Locked Bag 5102 Parramatta NSW 2124
www.police.nsw.gov.au

The Hon Yasmin Catley MP
Minister for Police and Counter-terrorism
Minister for the Hunter

NSW GOVERNMENT

Ref: MINS-522608304-20911
F/2025/43622

The Hon Tanya Plibersek MP
Minister for Social Services
Federal Member for Sydney
PO Box 2676
STRAWBERRY HILLS NSW 2012

Tanya.Plibersek.MP@aph.gov.au

Dear Minister,

Thank you for your correspondence on behalf of Mr Anthony Smith regarding allegations of identity theft and misconduct by police.

The NSW Government and the NSW Police Force (NSWPF) take all complaints regarding policing very seriously. Complaints against employees of the NSWPF are managed in accordance with Part 8A of the *Police Act 1990*. Independent oversight of this process is exercised by the Law Enforcement Conduct Commission.

I am advised that the allegations raised by Mr Smith have been fully investigated by the NSWPF's Kings Cross Police Area Command (PAC) on a number of occasions. Police have also engaged with Mr Smith over a period of time in relation to his concerns and he has been informed that there is insufficient evidence to substantiate claims of identity theft.

I am further advised that on 8 July 2025, an officer from Kings Cross PAC spoke with Mr Smith to further discuss his concerns, where he was provided with additional information on the outcome of the investigation by police.

Should Mr Smith have further concerns, please encourage him to contact Kings Cross PAC on (02) 8356 0099.

Thank you for writing about this matter.

Sincerely,

Yasmin Catley MP
Minister for Police and Counter-terrorism
Minister for the Hunter

52 Martin Place Sydney NSW 2000
GPO Box 5341 Sydney NSW 2001
02 7225 6100
nsw.gov.au/ministercatley

Ian Steptoe

From: John-Paul Brookes T1(f)
Sent: Wednesday, 20 Augus :
To: #SECRETARIAT
Subject: Minister's response - MINS-522608304-22693 - Alex Greenwich MP - Anthony Smith - Cybercrime Squad review into identity theft
Attachments: Smith Cybercrime Squad REP 250820 aml.pdf; Cybertrace Investigation - Impersonation and Harassment of Tony Smith - 2025 2 (1).pdf

Follow Up Flag: Follow up
Flag Status: Flagged

OFFICIAL

Hi Team

Can a Minister's response please be prepared in relation to the attached representation.
Any questions please let me know.
Kind regards
JP

John-Paul Brookes
Departmental Liaison Officer
Office of the Hon Yasmin Catley MP
Minister for Police and Counter-terrorism
Minister for the Hunter
M T1(f) **E** T1(f)
nsw.gov.au
52 Martin Place
Sydney NSW 2000

I acknowledge the traditional custodians of the land and pay respects to Elders past and present. I also acknowledge all the Aboriginal and Torres Strait Islander staff working with NSW Government at this time.
Please consider the environment before printing this email.

OFFICIAL

From: Alex Greenwich MP
Sent: Wednesday, 20 August 2025 3:00 PM
To: Catley Office Email
Subject: (Case Ref: AG58708)
Good Afternoon

Please see attached correspondence from Alex Greenwich MP.

Kind regards

Annie McCall
Electorate Officer
Alex Greenwich MP
Member for Sydney
T1(f)

alex greenwich
INDEPENDENT MEMBER FOR SYDNEY

20 August 2025

The Hon Yasmin Catley MP
Minister for Police and Counter-terrorism
GPO Box 5341
SYDNEY NSW 2001

Our ref: AG58708

Dear Minister

Request for matter to be reviewed by the Cybercrime Squad

I write on behalf of my constituent Anthony Smith of 801/281-283 Elizabeth Street, SYDNEY who is seeking a Cybercrime Squad review into identity theft, cyberstalking, and criminal impersonation of himself.

Mr Smith tells me that this situation has been ongoing since 2019 and shared with me correspondence from LECC (dated 20 September 2024) that cautioned him contacting LECC again "unless he had significant new and cogent information".

Mr Smith has provided the attached report by Cybertrace Pty Ltd dated 3 June 2025. In good faith and with his permission, I am providing this as new information which may lead to a resolution.

Could you please have Anthony's matter reviewed by the Cybercrime Squad and tell me what will be done to help him reach a satisfactory resolution?

Yours sincerely

Alex Greenwich
Member for Sydney

Attachment: Report by Cybertrace Pty Ltd dated 3 June 2025

Ground Floor, 21 Oxford St Darlinghurst NSW 2010
P 9267 3999 E sydney@parliament.nsw.gov.au alexgreenwich.com.au

Ian Steptoe

From: Caroline Shepherd
Sent: Thursday, 21 August 2025 14:15
To: #SCCCOMMAND
Cc: #DCOPICT
Subject: Advice request - Alex Greenwich MP obo Anthony Smith - Cybercrime Squad review into identity theft [SEC=OFFICIAL]
Attachments: Smith Cybercrime Squad REP 250820 aml.pdf; Cybertrace Investigation - Impersonation and Harassment of Tony Smith - 2025 2 (1).pdf

Importance: High

To	State Crime Command
Date due to Ministerial and Executive Services	**4 September 2025**
Topic	Identity theft / cyber crime
Correspondent/agency	Alex Greenwich MP obo Anthony Smith
Request	Please find attached correspondence for review and advice for Ministerial response.
RMS container	F/2025/55291
For more information, please contact	Caroline Shepherd

Thank you

NSW Police Force

Caroline Shepherd
Senior Ministerial Officer
Office of the Commissioner
Locked Bag 5102 Parramatta NSW 2124
E: T1(f) **M:** T1(f)

Pages 110 through 111 redacted for the following reasons:
- -
-T1(e), T1(f), T3(a), T3(b)

Ian Steptoe

From: Caroline Shepherd
Sent: Friday, 5 September 2025 09:56
To: #CMRreturns
Cc: #DCOPMETRO
Subject: Advice request - Alex Greenwich MP obo Anthony Smith - Cybercrime Squad review into identity theft [SEC=OFFICIAL]
Attachments: Smith Cybercrime Squad REP 250820 aml.pdf; Cybertrace Investigation - Impersonation and Harassment of Tony Smith - 2025 2 (1).pdf; SCC Response - MO - MINS-522608304-22693 - Alex Greenwich MP obo Anthony Smith - Cybercrime Squad review into identity theft.PDF

Importance: High

To	Central Metropolitan Region
Date due to Ministerial and Executive Services	**18 September 2025**
Topic	Identity theft / cyber crime
Correspondent/agency	Alex Greenwich MP obo Anthony Smith
Request	Please find attached correspondence for review and advice for Ministerial response. Note: Advice has been provided by SCC (pink attached).
RMS container	F/2025/55291
For more information, please contact	Caroline Shepherd

Thank you

NSW Police Force

Caroline Shepherd
Senior Ministerial Officer
Office of the Commissioner
Locked Bag 5102 Parramatta NSW 2124
E: T1(f) **M:** T1(f)

Pages 113 through 114 redacted for the following reasons:
- -
-T1(e), T1(f), T3(a), T3(b)

Ian Steptoe

From: #NO-REPLYMES
Sent: Thursday, 2 October 2025 09:35
To: sydney@parliament.nsw.gov.au
Subject: Reply to correspondence - F 2025 55291
Attachments: Ministerial response - Alex Greenwich MP obo Smith - F 2025 55291.pdf

This email address is not monitored for replies.

Please find attached a response to your correspondence.

To respond to the Office of the Minister for Police and Counter-terrorism and Minister for the Hunter online, please visit**:** **https://www.nsw.gov.au/nsw-government/ministers/minister-for-police-and-counter-terrorism**

To respond to the NSW Police Force online visit**:** https://www.police.nsw.gov.au/contact_us.

Regards

NSW Police Force.

NSW Police Force
Locked Bag 5102 Parramatta NSW 2124
www.police.nsw.gov.au

The Hon Yasmin Catley MP
Minister for Police and Counter-terrorism
Minister for the Hunter

Ref: MINS-522608304-22693
F/2025/55291

Mr Alex Greenwich MP
Member for Sydney
Ground Floor
21 Oxford Street
DARLINGHURST NSW 2010

sydney@parliament.nsw.gov.au

Dear Mr Greenwich,

Thank you for your correspondence on behalf of Mr Anthony Smith regarding allegations of identity theft.

I am advised that the allegations raised by Mr Smith have been fully investigated by the NSW Police Force (NSWPF) on a number of occasions. Police have also engaged with Mr Smith over a period of time in relation to his concerns and he has been informed that there is insufficient evidence to substantiate claims of identity theft.

I am further advised that an officer from the NSWPF's Kings Cross Police Area Command (PAC) recently spoke with Mr Smith to further discuss his concerns, where he was provided with additional information on the outcome of the investigation by police.

Should Mr Smith have further concerns, please encourage him to contact Kings Cross PAC on (02) 8356 0099.

Thank you for writing about this matter.

Sincerely,

Yasmin Catley MP
Minister for Police and Counter-terrorism
Minister for the Hunter

52 Martin Place Sydney NSW 2000
GPO Box 5341 Sydney NSW 2001

02 7225 6100
nsw.gov.au/ministercatley