INTERCEPTING MAIL DESTINATIONS.
*BLOCKED CONTACT TO ASSISTANCE ALL SERVICES

Australia Post

Our ref: 2000388

28 April 2020

[redacted]

Dear Ms Pearce,

I write with reference to your letter dated 11 March 2020 to Australia Post's Group Chief Executive Officer and Managing Director, Christine Holgate, regarding your requests for security measures. I have been asked to review and respond to the matter on Ms Holgate's behalf.

From the outset, I appreciate you taking the time to write with your request, and I can provide genuine assurance that our networks and facilities operate well-established security processes and procedures designed to safeguard items in transit.

Regarding increased security measures for sending and receiving of mail, unfortunately Australia Post is unable to implement the suggestions you have provided. While we do not have the capability, infrastructure, or dedicated personnel to design a restricted access scenario as you have suggested, Australia Post has existing transparent sending options.

Where there is need for transit and delivery visibility, we recommend the use of trackable products such as Registered Post, Express Post, or the new Domestic Letter with Tracking. If it assists, Delivery Confirmation and Person-to-person delivery can be added to some Registered Post articles. Full details on these products are available on our website.

While you can monitor a tracked items progress on our website, our Customer Contact Centre are also happy to assist with enquiries, and they can be reached by calling [redacted] or via the online options on our website.

Thank you for taking the time to bring this matter to the attention of our Group Chief Executive Officer and Managing Director. I trust the above information is of assistance.

Yours sincerely

[redacted]

Australia Post
GPO Box 1777 MELBOURNE VIC 3001
E: [redacted]
W: auspost.com.au

TELECOMMUNICATION SYSTEMS 2020 - 2021

POLICE INVOLVEMENT - FRAUDULENT ACTIVITY OBTAINED 2021 - GOV INVOLVEMENT

I reported the Fraudulent malicious Activity of the newly created business account to Joshua Adams, Business Consultant, Telstra Store, Kadina who proceeded to file a report to the Fraud Department and requested an investigation into the activity - Refer to Telstra Report dated 1/10/2020
I received no reply or response from this report.
The Fraudulent and malicious Activity continued and escalated.

On the 25/03/2021 I reported the activity again to Joshua Adams, Business Consultant, Telstra Store, Kadina and reported that I had not received any contact from the Fraud Department concerning the report that he had submitted. I requested a change of mobile phone number with the account still having Restricted Access applied. Joshua Adams proceeded to change the mobile phone number and did a check to ensure that the new number that I had been given was a newly created number that had not been circulated before my use, to ensure that the same activity would not occur and if it did would be seen as suspicious activity continued.

On the 25/03/2021 I reported the Fraudulent Malicious activity to Isobelle Oppelear, Manager, Telstra Store, Kadina who proceeded to file a report to a higher authority, requesting an investigation with the higher authority of the Fraud Division or CEO of Telstra, due to ongoing issues over a 10 year period of continuous Fraudulent Activity. - Refer to Letter addressed to Isobelle Oppelear, Manager - Refer to document filed report and Case ID number
I received contact from Telstra higher authority but missed the call and am waiting for the second contact, to ring me back as informed in the voice recorded message left on my mobile phone to discuss the issue.

On the 13th April 2021 I sent a letter addressed to the CEO of Telstra Head Office, Mr Andrew Penn, Melbourne, Victoria from the Norwood Post Office branch, Adelaide informing the CEO of the continuous Fraudulent Malicious Activity that had been occurring in my personal and newly created business account with Restricted Access, and requested a thorough investigation into the activity and provided the documented evidence of the activity that had been occurring in all servers and over a long period of time, and following re-location and change of details
Refer to letter addressed to CEO - Mr Andrew Penn - Telstra Head Office, Melbourne
Specific Targeting of an Individual - Every location, re-location, changed servers and personal details, including change of phone numbers - Pattern of Illegal Activity

CEO - REPLY - REMOTE ACCESS - GOV + POLICE

Ron - Telstra Head Office - 4th May 2021 - Ph: [redacted]
I received phone contact from Ron, Telstra Head Office following the submitted letter to Mr Andrew Penn, CEO of Telstra Head Office - Recorded Phone call.
I was informed that the reports that had been submitted over a 10 year period in Telecommunication Systems concerning continuous ongoing Fraudulent Activity in my accounts, following Restricted Access applied, change of phone numbers, change of details personal and business, change of servers and relocation was identified as Government and Police Sources Remotely Accessing servers, accounts and computer hardware to result in the Fraudulent activity that had been occurring, which included blocked contact, altered and blocked messages, blocked access to internet services, websites and contacts, impersonating of companies, unusual messages and phone calls from unknown people, blocked contact and altered messages to my children, as informed by my children and resulted in isolation in 2014 - 2016 Extreme Sexual Targeting, Police Targeting and detention. This information confirmed the details obtained in 2016 Origin Electricity account that incurred an Excessive Rise in billing that remained unexplained and resulted in the barcode being scanned as a Police Source causing the Fraudulent Activity. Townsville CC Parking Fines (Queensland Police Source).
The source of the Continuous Illegal Activity has now been identified as Government and Police Specific Targeting of an Individual over a 27 year period which resulted in the 2017 Murder to Appear as Suicide by medication as a result of Police Targeting Detention in Glenside Mental Health Facility

INTERNET - COMPUTER SYSTEMS - TOSHIBA LAPTOP.

7/13/2020 MICROSOFT INVOLVEMENT Mail - [redacted] - Outlook STOLEN PHOTO.

POLICE INVOLVEMENT - COMPUTER HACKING

2020 ACA-2020-000415 [SEC=OFFICIAL] REMOTE ACCESS

Cyber Abuse <[redacted]> CAUSE OF ILLEGAL FRAUDULENT

Mon 4/05/2020 12:58 PM AND MALICIOUS ACTIVITY

To: [redacted] BOTH COMPUTER SYSTEM

Cc: Cyber Abuse <[redacted]>

1 attachments (2 MB)

Cyber_abuse_Resource Sheet.pdf;

Dear [redacted]

Thank you for your recent enquiry, and we are sorry to hear how this is affecting you.

eSafety and Adult Cyber Abuse

The eSafety Commissioner's (eSafety's) primary role in dealing with cyberbullying complaints is to assist with the rapid removal of cyberbullying material targeted at Australian children, on social media services.

Please be aware that eSafety, therefore, has **no legislative power to investigate** adult cyber abuse complaints, formally. However, we do work to guide people where we can and provide advice on what they can do themselves.

In the most **serious cases**, we will use our existing relationships and escalation pathways with social media services to effect take-down of harmful material that is considered to be serious cyber abuse in nature or, where required, we will refer the matter to law enforcement.

Digital surveillance - IDENTIFIED AS ILLEGAL SURVEILLANCE RESULTING IN ILLEGAL ACTIVITY

Your situation sounds like it may be digital surveillance, which is not an area we generally handle or have experience in. You may wish to approach your email (and any other relevant) service provider about the situation.

You may also wish engage an IT consultant to assist you in this matter or a cyber digital forensic expert to assist you further and we'd encourage you to consider doing this in the meantime.

Reporting to police

If you wish to pursue this or to make a formal report to police, the following steps may help you prepare:

- Prepare a timeline of what has taken place
- Place any screenshots you have in a word document (provide a summary below each image explaining what the screenshot relates to)
- Provide copies of any URL's you may have (you can obtain the URL by copying and pasting the URL address from your browser address bar)
- If you believe you know who the person is that is targeting you online, provide as much detail about the person.

I have attached our Adult Cyber Abuse Resource sheet which contains useful eSafety and support links. You may want to reach out to support services to help you in this difficult time.

We have now finalised your matter for now and hope the above information assists you.

Regards,

Cyber Abuse Team

Service Ticket #621581 - [redacted] - Email Hack - 0400404658

Pit Stop Technologies <[redacted]>

Thu 9/07/2020 9:24 AM

To: [redacted]

Hello Jacqueline,

Service Ticket # 621581, has been completed. We hope that you are satisfied with the service provided. If you do not believe this ticket has been complete or have concerns, please respond to this email so we can address your queries.

Thank you,
Pit Stop Technologies Team
[redacted]
www.pit.net.au

PIT STOP TECHNOLOGIES
KEEPING YOUR IT ON TRACK

Ticket #: 621581 **Status:** Complete

Summary: [redacted] - Email Hack - 0400404658

Service Record #621581
Summary: [redacted] Email Hack - 0400404658
Company: [redacted]
Contact: [redacted]
Phone: [redacted]