
Cyber Security and Fraud

BT Fraud and Financial Crime

Detect | Deter | Disrupt

Financial Crime Centre of Excellence



- Fraud typologies
- Fraud prevention and detection
- What to do after a fraud
- Case study – Superannuation fraud
- Data as a commodity
- Fraud in financial crime
- BT case study
- Questions



Fraud Typologies - What does Fraud look like?



❑ Fraud is defined in the Criminal Code of Australia as 'dishonestly obtaining a benefit, or causing a loss, by deception or other means'

❑ Fraud is an act of intentional deception designed to exploit a victim. Fraud comes in many different forms with varying levels of complexity, here are some examples of fraud and fraud-related financial crimes you may see or experience

Recent estimates by the Commonwealth Attorney General's Department indicate that identity crime costs Australia upwards of \$1.6 billion per year, with the majority lost by individuals through credit card fraud, identity theft and scams. Identity crime continues to be a key enabler of serious and organised crime, which in turn costs Australia around \$15 billion annually (source: AFP Identity Crime website)

Typologies for theft of Personal Identification Information (PII) which can lead to Identity Fraud:

Theft of Identity Documents	Internet Scams	Virus / Malware	Telemarketing Scams	Hacking / Data Breach	Social Media
<p>Theft of Mail articles, wallets, bags and purses</p> <p><i>Identity theft is a type of fraud that involves using someone else's identity to steal money or gain other benefits.</i></p>	<ul style="list-style-type: none"> Phishing emails and texts Spoofing sites to replicate banking and payment sites <p><i>Phishing scams are attempts by scammers to trick you into giving out your personal information such as your bank account numbers, passwords and credit card numbers.</i></p>	<p>Malicious computer programs such as malware or spyware Ransomware</p> <p><i>Malware tricks you into installing software that allows scammers to access your files and track what you are doing, while ransomware demands payment to 'unlock' your computer or files.</i></p>	<ul style="list-style-type: none"> Cold Calls purporting to be from a Bank or Authority body Remote access scams <p><i>Remote access scams try to convince you that you have a computer or internet problem and that you need to buy new software to fix the problem.</i></p>	<p>Hacking of websites or business servers containing personal information data bases</p> <p><i>Hacking occurs when a scammer gains access to your personal information by using technology to break into your computer, mobile device or network.</i></p>	<p>Fake online social media profiles</p> <p><i>Scammers use all kinds of sneaky approaches to steal your personal details. Once obtained, they can use your identity to commit fraudulent activities such as using your credit card or opening a bank account.</i></p>

- Application Fraud
- Phone Fraud
- Credit Card Fraud
- Cheque Fraud
- Merchant Fraud
- Cybercrime
- Identity Fraud
- Scams
- Malpractice
- Signature Fraud

Question 1

What kind of Fraud consists of hacking websites, business servers and information data bases ?

- A. Theft of Identity Documents
- B. Hacking Data Breach
- C. Telemarketing Scams

What is identity fraud?



Given there are so many different types of fraud it can be hard to know exactly what to look out for.

The most common type of fraud experienced in the wealth management space is Identity Fraud.

There are 2 types of identity theft:

- ❑ The theft of personal identity information and related financial information; and
- ❑ Assuming another identity for fraudulent purposes.







Even if only a small amount of personal information is obtained, perpetrators often use open source information (e.g. social media) to piece together other details such as date of birth, frequently attended locations, contact details etc. They can then use this information to impersonate their victim and access accounts, apply for credit, etc.



Fraud Facts — in 2022, ACCC reported \$3.1B was lost to scams in Australia

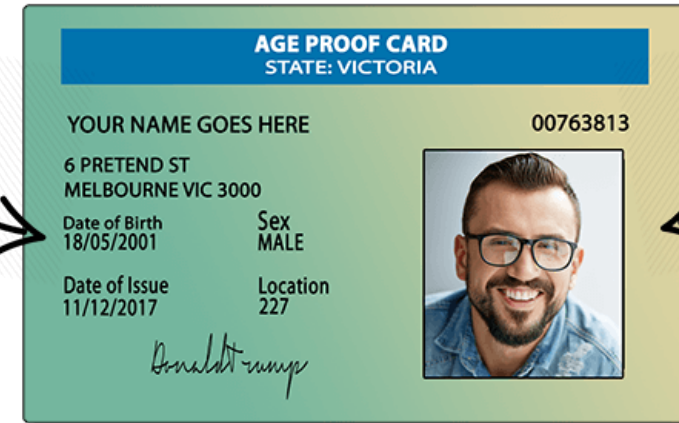
ID documents have come a long way over the past couple of decades. Many documents now contain security features such as holograms and moving graphics to help prevent counterfeit production.

HOWEVER, in the financial services industry, we often come across certified copies of original documents. This means that we need to be extra vigilant as we cannot rely on seeing the original document. Some things to look out for are:

-  Irregularities in the documents such as different fonts and font sizes, spelling errors, borders or lines where there should be none.
-  Ensure that the photo lines up correctly and does not look out of place.
-  Ensure the photo does not depict eyewear or face coverings, and that the person in the photo is looking straight ahead.
-  The photo should be taken against a blank background.
-  Ensure the person in the photo matches the profile of the individual (i.e.: age, ethnicity etc)
-  Where multiple forms of photo ID has been provided, is the person in the photograph on each the same individual?

customise your own details

Your face goes here



Question 2

What does the acronym PII stand for?

- A. Professional Industry Information
- B. Public Information Insights
- C. Personal Identification Information

What is BT doing?



- 2 Factor Authentication
- Push notifications
- Transaction Monitoring – including rules around known fraud indicators
- Notification to Advisers of important changes to client details
- Uplift in Enhanced Customer Due Diligence, ensuring all data is up to date
- Regular review of cyber trends and shocks as input for updates to our security measures
- Uplift in fraud awareness training
- Regular and mandatory training on IT security
- Simulated phishing emails to ensure staff maintain awareness
- Regular review and assessments of our risks and controls



HOW YOU CAN HELP

- Ensure you are capturing accurate customer details – ensure name, DOB, address matches identification *exactly*
- Look out for red flags – ensure you double check customer's email address if acting on email instruction, ensure beneficiary account details are correct and match your records, be aware of things like multiple changes to a customer profile in a short period of time
- Confirm information and changes directly with the customer
- Talk to your customers about cyber security and keeping their systems/devices protected – don't wait until it's too late to have those conversations
- Ensure YOUR systems are safe and keep security programs up-to-date
- Review the Australian Cyber Security Centre's 'Exercise in a Box'

- Ensure you are running high-quality anti-virus / anti-spyware / anti-malware programs and keep them up to date
- Never click on links in unexpected emails or text messages; don't open attachments unless you are sure of source
- Do not connect to free public wifi networks
- NEVER share user names or passwords, and never record them anywhere
- Do not give out personal information unless secure – including social media
- Limit social media connections to people you know in real life
- Review financial statements often
- Ensure passwords are not easy to guess
- Use different passwords for different systems / applications



After Identity Fraud – What to Do



- ✓ Contact bank/financial services provider to have additional security measures added where possible (i.e. account stopped, passwords reset or added, secret questions, alerts on profiles etc)
- ✓ Change passwords on devices and accounts
- ✓ Consider replacing credit cards where required
- ✓ Have personal devices cleaned by a professional
- ✓ Report to law enforcement
- ✓ Check your credit report
- ✓ Subscribe to credit alerts
- ✓ Contact ID Care



Regulator and Law Enforcement - 2019 Cyber Investigation

What did the activity look like?



A 24 year old woman from VIC admitted to playing a central role in an international fraud syndicate "Team Awesome" which targeted superannuation and share trading accounts



The Perpetrator set up a phishing scam to access account login details, and bought other victim details off dark web

Business were targeted with admin, HR or bookkeeper usernames in the hope they would give her access to superannuation acct details and identification documents.

Used victim details to set up emails, phones, and bank accounts.



Money was then withdrawn from victims' superannuation & share trading accounts.



More than \$2.5M was laundered through Hong Kong via untraceable valuables, then sold. The proceeds were then distributed to offenders in cryptocurrency

Police found 1400 documents on her computer. She admitted to manipulating ID documents to change names or dates of birth and then stamping them with a false certification stamp

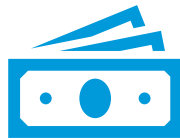


Victim details used to withdraw funds from accounts / sell shares, with proceeds deposited to newly opened bank accounts. Debit cards were then sent to false addresses and used by people in Hong Kong to launder proceeds.

There were 5 others who are known only by aliases – she is only person to date to be caught and charged



Arrested in April 2019 at Melbourne airport while returning from Turkey. Pleaded guilty to 2 x conspiracy to defraud charges and one charge of conspiring to deal in proceeds of crime.



- ❑ 2019: A 21-year-old Melbourne woman appeared in Court as part of investigations into a major fraud and identity theft syndicate, which resulted in alleged thefts from the superannuation and share trading accounts of innocent victims worth of millions of dollars
- ❑ ASIC and the AFP allege the woman worked as part of a syndicate which used fraudulently-obtained identities to commit large-scale online fraud.
- ❑ ASIC and the AFP further allege the syndicate laundered the stolen funds through an overseas contact to purchase untraceable assets.

Data as a commodity– How important is it?

Source: AUSTRAC Superannuation Threat Update 2022

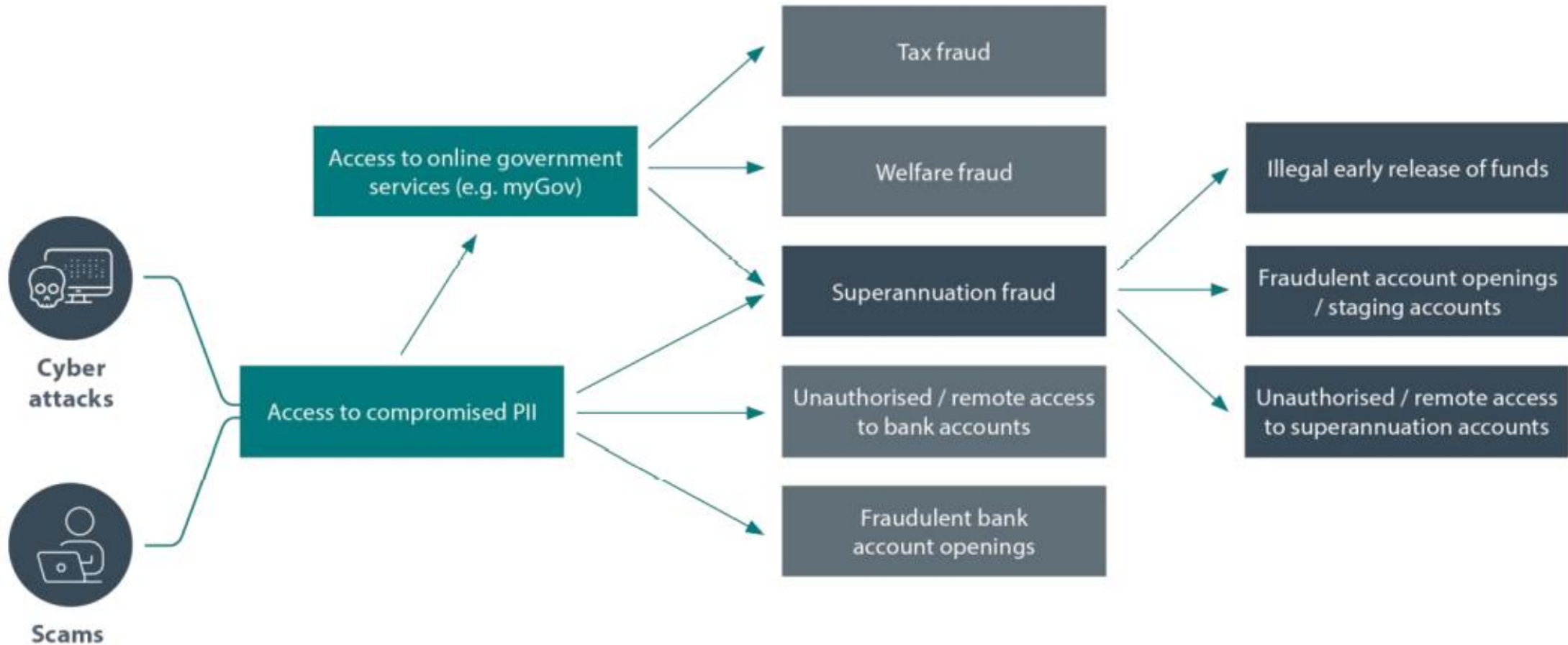


Figure 5: Demonstrates how the access to compromised PII can contribute to the exploitation of various financial services.

Question 3

Finish this sentence: Data as a commodity is commonly compromised through Scams and _____?

- A. Media
- B. Cyber attacks
- C. Police notification

Data Breaches in Australia 2022 / 2023

– Source: <https://www.webberinsurance.com.au/data-breaches-list>



<p>APRIL</p> <ul style="list-style-type: none"> TAFE <p>MARCH</p> <ul style="list-style-type: none"> Canberra Health Services iD Tech Rio Tinto QIMR Berghofer Latitude NSW Health CBA <p>FEBRUARY</p> <ul style="list-style-type: none"> The Good Guys Guardian Australia JD Sports <p>JANUARY</p> <ul style="list-style-type: none"> GoTo Mount Lilydale Mercy College 	<ul style="list-style-type: none"> QUT Paypal Norton LifeLock <p>DECEMBER</p> <ul style="list-style-type: none"> Fire Rescue Victoria LastPass TPG Telecom State Office of Victoria LJ Hooker Telstra <p>NOVEMBER</p> <ul style="list-style-type: none"> Twitter WhatsApp The Smith Family Harcourts Melbourne City PNORS Technology Group 	<p>BWX (Flora & Fauna)</p> <p>OCTOBER</p> <ul style="list-style-type: none"> SSKB Microsoft AFP Vinomofu Medibank Woolworths MyDeal <p>SEPTEMBER</p> <ul style="list-style-type: none"> North Face Optus Uber Freemantle Football Club TikTok <p>AUGUST</p> <ul style="list-style-type: none"> LastPass DoorDash Facebook WA Health 	<ul style="list-style-type: none"> Cisco Twitter University of WA <p>JULY</p> <ul style="list-style-type: none"> Neopets Uber Perth Festival, Black Swan State Theatre Company VIC Government Woolworths Marriott Mangatoon China Police Deakin University AMD OpenSea <p>JUNE</p> <ul style="list-style-type: none"> iCare 	<p>MAY</p> <ul style="list-style-type: none"> Department of Home Affairs NDIS Spirit Super APAC Facebook SA Government National Tertiary Education Union Transport for NSW <p>APRIL</p> <ul style="list-style-type: none"> SuperVPN, GeckoVPN, ChatVPN Coca-Cola Panasonic Block (ASX:SQ2)
---	--	--	--	--

Data Breach in the Media



- ❑ In mid-March, Latitude announced they had fallen victim to a cyber attack, where 328,000 of their Australian and New Zealand based customers' identities had been compromised
- ❑ Latitude announced that they believed the attacker appeared to have used the login credentials of an employee to steal personal information that was held by two other service providers
- ❑ It has been reported that approximately 103,000 identification documents, 97% of which are copies of drivers licences, were stolen from a first service provider. A further 225,000 customer records are believed to have also been stolen from a second service provider
- ❑ It is believed that the hack originated from a major vendor used by Latitude (unnamed)
- ❑ Latitude reported they initially noticed 'unusual activity' on their systems, however by the time they realised it was a cyber security breach and took action accordingly, it was too late as employee login credentials had already been compromised and access gained to the two service providers



CASE STUDY - Advisor Experience and BT Response



- ❑ Information received via a customer, who Police had contacted after finding a notebook during a search warrant, which contained his personal information, including his BT account details
- ❑ On further investigation it was identified that there was believed to have been a compromise via a Financial Planner's office, which had been closed for approximately 3 years at that time. A number of customers had their personal details compromised.
- ❑ Advice received that the perpetrators were compromising the victims' myGov accounts
- ❑ BT implemented targeted monitoring of the customers affected, which included writing specific alert rules to target certain behaviours and transactions. Alerts were directed to a number of key personnel, who would then contact the relevant Advisor if and when an alert triggered, in order to confirm the veracity of activity.
- ❑ BT were able to work with law enforcement to obtain specific information to assist in the monitoring of activity.



Thank You.