Identity & Cyber Security Community Aftermath Report 2018

About this Report

This report provides a summary of impacts identity and cyber-related crimes had on the Australian community throughout calendar year 2017.

It aims to inform readers about the experiences of everyday Australians with crimes that impact their personal information, wealth, and well-being.

Unlike other public reporting, IDCARE's Aftermath Report 2018 captures unfiltered views from our community on the good, the bad and the ugly in terms of prevention, detection, preparedness and response. IDCARE does not impose arbitrary thresholds nor is it constrained by legislative remit in supporting those who engage our services. Matters that present from clients are incredibly broad, including both online and offline scams and cybercrimes.

Change Opportunities for the Better

Our insights from 2017 present a number of change opportunities, including:

- Advancing law enforcement's efforts to upskill and pursue cybercriminals and offshore scammers targeting Australia;
- Ensuring key government credential issuers enhance their agility and relevance of response efforts to address community concerns and needs;
- Building and connecting response networks across industry and government;
- Exploring legislative, regulatory and market-driven models that influences market behaviour in avoiding the enabling of cybercrime and related scams;
- Building the evidence base on what is really impacting on our community when it comes to identity and cyber-related crimes.

About IDCARE

IDCARE was launched by the Commonwealth and New Zealand Governments in 2014 and 2015 respectively as a Trans-Tasman national identity and cyber support service for the community. Our organisation is a registered Australian not-for-profit charity and our frontline services are free to the community..

IDCARE is not a reporting entity, like ScamWatch or ACORN, rather it is a supporting entity that receives referrals from over 200 organisations annually, including ScamWatch and ACORN. The vast majority of these contacts result in the provision of specialist identity and cyber security counselling and pragmatic support. The largest referrer to IDCARE in 2017 was the Commonwealth government, and in particular, the Department of Human Services, the ACCC, ACORN, and the Australian Taxation Office.

Australian client experiences have been analysed and presented in this report. These clients reside in every electorate and their stories present a rich picture of Australia's capacity to prevent and respond to what is an enduring challenge for the economy's digitisation and underlying innovation.

Member and Advisor Briefings

IDCARE's Managing Director would welcome the opportunity to answer any questions or provide further briefing on this information. Bookings may be made by emailing <contact@idcare.org> or by calling 07 5373 0406.

Identity & Cyber Security Community Aftermath Report 2018 – New South Wales

In 2017 IDCARE's community services responded to **14,613 calls** from residents in New South Wales, investing around **11,256 hours** in specialist counselling support. The second part of this report captures key statistics from this electorate, providing unique insights on how identity and cyber crimes are impacting members of this community.

Impacted Residents

1 in **1,001** residents aged 15 years and over engaged IDCARE during 2017.

48% of clients were aged between 25 and 44 years old.

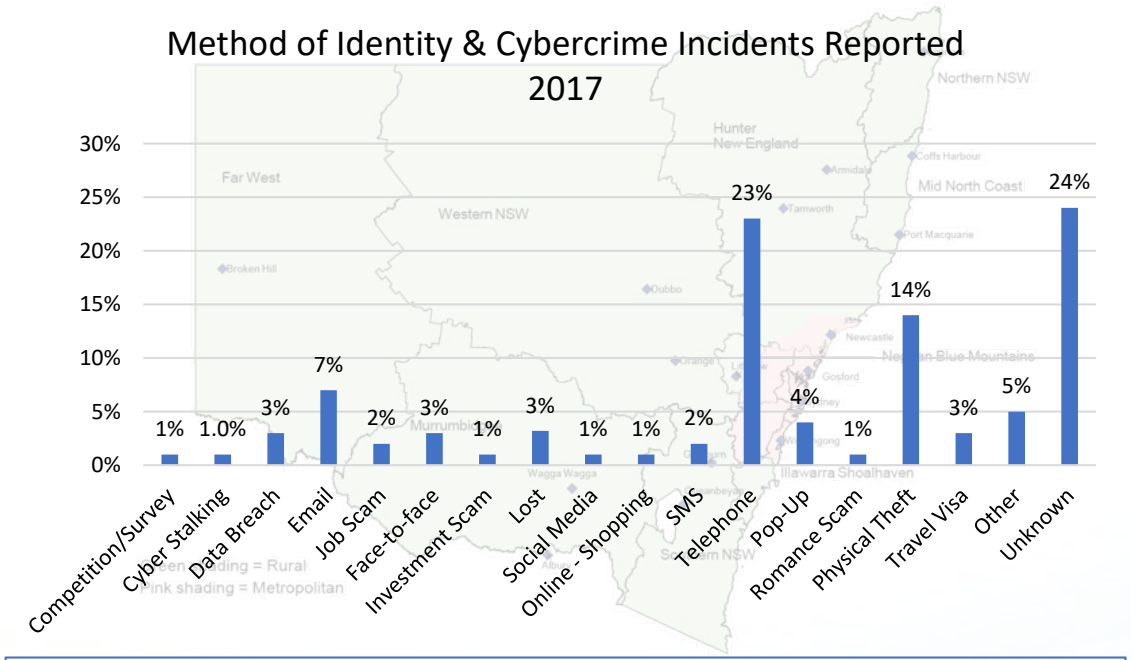
57% identified as **female**.

Detecting and Finding Help

65.8% of residents were the first to detect their cyber and identity security event (not an organisation).

53.8% of clients were referred to IDCARE by an organisation. Of these referrals, approximately **44%** came from Commonwealth agencies.

It took residents on average **18.7 days** to detect their incident, with an average loss of approximately **$1,942**.



Response Journey

The Commonwealth was rated by residents as the best responders to identity and cyber crimes (averaging **6.3 / 10** for satisfaction). The worst performers were telecommunication companies (averaging **3.8 / 10** for satisfaction). IDCARE's client satisfaction score for residents was **9.4/10**.

On average residents made **14.1** contacts to **9.3** separate organisations in response to their incident over an average of **24.58** non-consecutive hours.

Crime Insights

It took on average **12.9 days** for the criminals to commit further crimes following the initial identity or related cybercrime event.

Around **one third** of residents experienced the misuse of their identity credentials and a little over **one in four** did not know how the initial crime occurred.

Where the compromise event is known, **30.4%** of residents experienced a **telephone scam, 18.5%** of residents experienced a physical theft of device and/or credential(s), and **9.6%** experienced an **email related scam**.

49.2% experienced an event where the criminal was believed to originate from offshore.