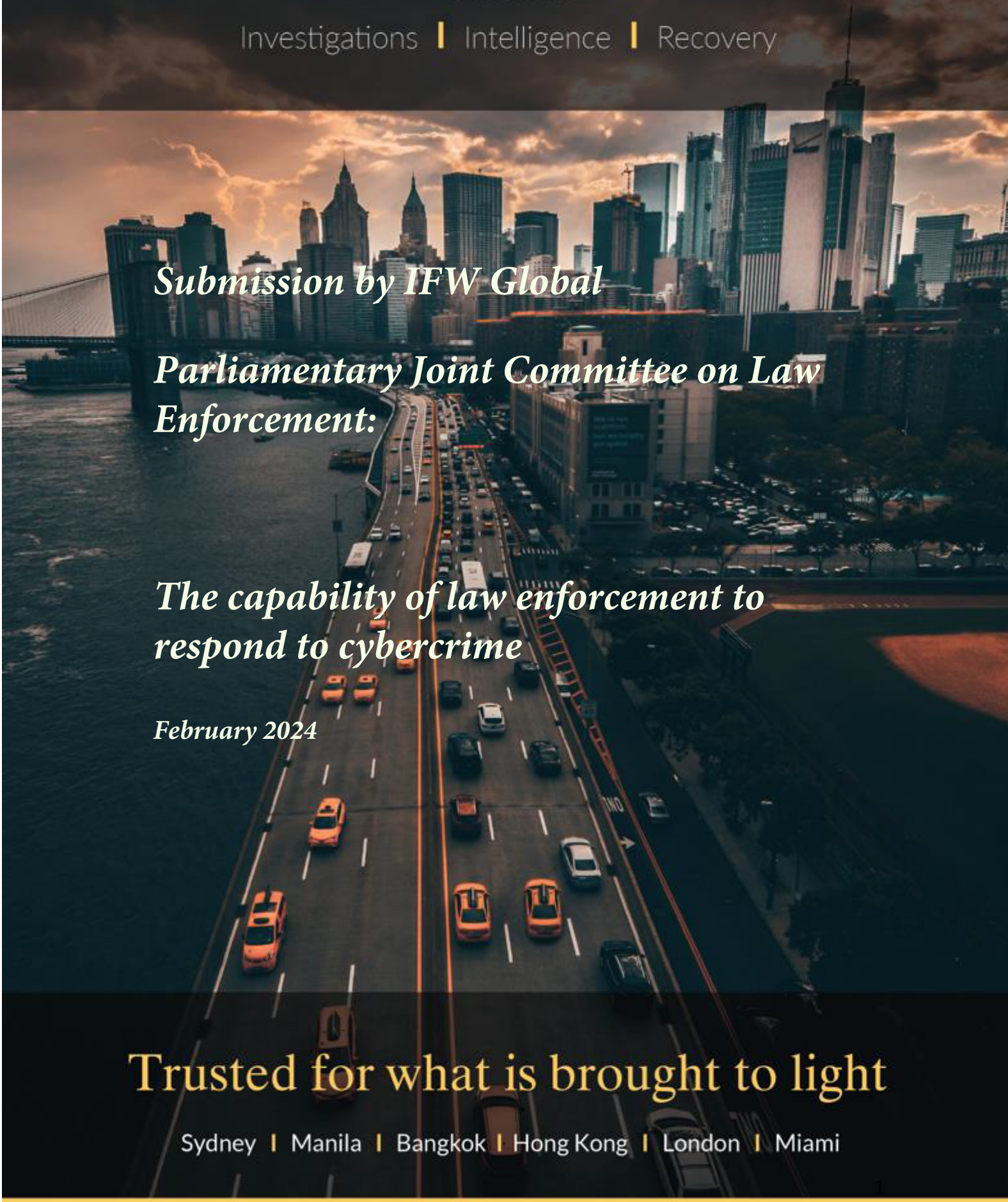
IFW

GLOBAL

Investigations | Intelligence | Recovery



Submission by IFW Global

Parliamentary Joint Committee on Law Enforcement:

The capability of law enforcement to respond to cybercrime

February 2024

Trusted for what is brought to light

Sydney | Manila | Bangkok | Hong Kong | London | Miami

IFW
GLOBAL

Investigations | Intelligence | Recovery

Background

Founded in 2007, IFW Global Investigations Pty Ltd (**IFW**) is a private criminal investigation and intelligence firm licensed by New South Wales Police under the Security Industry Act 1997 and by the State of Florida in the United States.

IFW represents private and corporate victims of fraud, providing investigative services geared to combatting complex criminal activities and pursuing asset recovery for clients in foreign jurisdictions.

The firm specialises in investigating online scams, investment frauds and cybercrime and has a track record of recovering millions of dollars from foreign-based cybercrime groups.

IFW deploys specialist technical staff and contractors for intelligence gathering, data analytics, digital forensics, cryptocurrency tracing, covert engagement, and lawful surveillance.

IFW works closely with overseas law enforcement, anti-corruption, and regulatory agencies as well as other private sector investigation and intelligence firms. It maintains a network of close contacts and sources in relevant industries including embedded human sources and whistleblowers in multiple countries.

Terms of reference of Inquiry

1. Existing law enforcement capabilities in the detection, investigation, and prosecution of cybercrime, including both cyber-dependent crimes and cyber-enabled crimes;
2. International, federal, and jurisdictional coordination law enforcement mechanisms to investigate cybercrimes and share information related to emerging threats;
3. Coordination efforts across law enforcement, non-government, and private sector organisations to respond to the conduct of cybercrimes and risks of cybercrime
4. Emerging cybercrime threats and challenges affecting Australian entities and individuals, including the scale and scope of cybercrimes conducted in Australia or against Australians;
5. The opportunities and challenges of the existing legislative framework in supporting law enforcement to investigate and act upon instances of cybercrime;
6. Prevention and education approaches and strategies to reduce the prevalence of victimisation through cybercrime; and
7. other related matters.

IFW
GLOBAL

Executive Summary

I am pleased to provide this submission on behalf of IFW Global Investigations Pty Ltd (**IFW**) to the Parliamentary Joint Committee on Law Enforcement Inquiry into the capability of law enforcement to respond to cybercrime. This submission is in two parts. The first part being the introduction and executive summary from me, the executive chairman of IFW and the second part being a detailed submission from Mr Mark Solomons addressing the specific terms of reference for this enquiry. Mr Solomons is an award-winning investigative journalist and licensed private investigator employed by IFW as a senior investigator.

Cybercrime has transformed into a complex and widespread transnational menace demanding immediate action and pre-emptive measures from the Australian government. There have been some failures to address adequately aspects of this serious crime problem, especially as it relates to online investment fraud and scams targeting Australian citizens.

In 2022 in Australia, more than $3.1 billion was siphoned from Australian victims by organised and sophisticated criminal fraud syndicates based overseas, an 80 per cent increase over 2021. Some of the most costly scams on an individual basis have been investment frauds of various types and this has fraud type has shown rapid growth.

Such scams include online foreign exchange trading, securities fraud, cryptocurrency trading and investment and other online "get rich" schemes, as well as term deposit and bank bond scams. This has come alongside rapid growth of "pig butchering" scams by Chinese organised crime groups, which use social media apps and romance bait to lure victims into investing into bogus cryptocurrency exchanges and trading websites.

These forms of cyber-enabled crime are orchestrated by industrial-sized crime syndicates operating overseas from concealed locations. A large proportion of the offenders targeting Australia are Israeli crime groups operating call centres in Southeast Asia and Eastern Europe. There is also intelligence suggesting some overlap between Israeli and Chinese organised crime groups.

These criminal groups establish offices and compounds and obscure their true whereabouts using Virtual Private Networks and Voice Over Internet Protocol phone numbers.

The crime bosses and leaders manage their operations as highly structured businesses.

In some instances, the scale of these fraudulent schemes is staggering, involving hundreds or even thousands of employees complicit in the scams. Such elaborate setups enable these criminal enterprises to perpetrate fraud on a massive scale, leveraging the anonymity and reach afforded by digital technologies.

IFW
GLOBAL

Artificial intelligence (AI) presents a new and significant future threat to Australia due to its actual and potential misuse by malicious actors for criminal purposes. As AI technology continues to advance, its potential to facilitate various forms of cybercrime, including data breaches, identity theft, financial fraud, and the dissemination of disinformation, grows.

IFW is already investigating cases involving deepfakes and AI-generated fraud. While law enforcement agencies play a vital role in combating AI-driven crime, addressing this complex challenge requires a collaborative and multifaceted approach involving government, industry, academia, and the public.

By working together, Australia can better prepare itself to confront the evolving landscape of cyber and AI-enabled criminal activities and safeguard its citizens, infrastructure, and digital economy from emerging threats.

I believe it is imperative that the government takes swift action to reform the way law enforcement agencies address these issues. The current deficiencies in experience and resources within some law enforcement units significantly hinder their capacity to adequately investigate and prosecute cyber offenders.

To address these challenges, establishing public-private partnerships with specialised firms in the private sector is paramount. There are many public firms that possess the requisite expertise and a proven track record in investigating and combating cybercrime.

By leveraging the capabilities of private-sector partners, law enforcement agencies can enhance their effectiveness in addressing cyber threats, better protecting individuals, businesses, and national security interests in an increasingly digital world.

The threat of cybercrime has left individuals and businesses vulnerable to increasingly sophisticated cybercriminal tactics. Victims of online investment fraud are facing devastating financial consequences, with losses spreading across diverse sectors of the Australian economy.

The escalating issue of cybercrime, particularly cyber-enabled investment fraud, has been inadequately addressed by both state and federal law enforcement agencies in Australia. This has resulted in a loss of public confidence in law enforcement capabilities and, more significantly, has allowed catastrophic financial losses to victims across the country.

To address the urgent need for change, I strongly recommend that the Australian government implement the following measures:

1. **Awareness and Education**: Increased awareness among the public, law enforcement agencies, and policymakers about the potential risks associated with cyber and AI-driven crime is essential.

IFW
GLOBAL

Education programs can help individuals and organizations recognise the signs of cyber and AI-based threats and adopt proactive measures to mitigate risks.

2. **Regulatory Frameworks**: Robust regulatory frameworks are needed to govern the development, deployment, and use of cyber and AI technologies. These regulations should address issues such as data privacy, algorithmic accountability, and transparency in AI systems to prevent their exploitation for criminal purposes.

3. **Capacity Building**: Law enforcement agencies need to enhance their capabilities to detect, investigate, and prosecute cyber and AI-driven crimes effectively and across international borders. This may require specialised training programs overseas, the recruitment of experts in cybercrime, AI and cybersecurity, and the establishment of dedicated units focused on combating technologically sophisticated threats coming from international crime groups.

4. **Public-Private Partnerships**: Collaboration between law enforcement agencies, industry experts, and the private sector is crucial in addressing cyber and AI-driven crime effectively. Private-sector entities often possess valuable expertise, resources, technologies, and international law enforcement relationships and contacts that can complement the efforts of law enforcement in combating emerging threats.

5. **Technological Solutions**: The development and deployment of advanced technological solutions, such as AI-powered cybersecurity tools and threat intelligence platforms, can help identify and mitigate AI-driven threats in real-time in the future.

It is paramount that swift and decisive action be taken to restore public confidence in the government's ability to address cybercrime effectively. The financial losses and personal hardships experienced by victims demand a proactive and collaborative approach that integrates the expertise of both public and private sectors.

Thank you for your attention to this critical matter. I trust that the Australian Law Enforcement Committee will prioritise the necessary reforms to safeguard the nation against the escalating threat of cybercrime.

Sincerely,

Ken Gamble
Executive Chairman
IFW Global Investigations Pty Ltd

IFW
GLOBAL

Submission by Mark Solomons, senior investigator

Mark Solomons is a licensed private investigator working as a senior investigator for IFW, specialising in multinational cybercrime and large-scale fraud investigations.

1. **Existing law enforcement capabilities in the detection, investigation, and prosecution of cybercrime, including both cyber-dependent crimes and cyber-enabled crimes**

IFW's focus of work is investigating cyber-*enabled* crimes, where an underlying fraud involving a fake or rigged investment or trading scheme or other alleged offence such as a romance scam or extortion attempt is facilitated by communications technologies.

These are mainly traditional scams that have harnessed the internet and used other novel technologies, such as cryptocurrency for laundering the proceeds, to become more efficient and profitable.

But the sheer scale of the scams and the sophistication and professionalism of the syndicates running them has come about not just because of technology. It has been helped along very nicely by a global failure to identify or tackle the offending.

Australia bears some responsibility for this and is reaping the effects. Australia, New Zealand, Canada, the UK, and Sweden are among a small group of wealthy countries disproportionately targeted by scam syndicates. The syndicate masterminds know that the risk of detection, investigation and prosecution by these countries is low and heavily outweighed by the potential rewards.

Data from Chainalysis shows Australia and New Zealand were in the top rank globally in terms of scam revenue per capita for investment scams in 2022, alongside Canada, Scandinavian countries, and parts of South America.

https://go.chainalysis.com/rs/503-FAP-074/images/Crypto_Crime_Report_2023.pdf

The cyber component of cyber-enabled crime, while not essential for the offence type, is the key to its detection and investigation. The technical competence of law enforcement and regulatory agencies is therefore crucial, and unfortunately in Australia and many other targeted countries it lags well behind that of the criminals.

There has also been misdirection of existing technical competencies. Australian government policy and law enforcement resourcing at the critical federal level has focused on cyber-*dependent* crime, such as ransomware attacks, phishing, hacking, and online abuse. This has led to a failure to check a significant increase in the incidence of cyber-*enabled* crime.

IFW
GLOBAL

Australians are effectively paying the price for structural, cultural and policy deficiencies in Australian law enforcement and regulation that have made Australia one of the most rewarding territories in the world for overseas scammers.

Evidence obtained by IFW from inside the syndicates shows that Australia is the number one target for cryptocurrency scams operated by Israeli-run groups. These groups dominate such offending globally alongside so-called "pig butchering" type scams run from south-east Asia that until recently have focused mainly on Chinese-speaking populations.

A multilayered, multi-billion-dollar scamming network linked to Israeli masterminds, with operations in Cyprus and across Eastern Europe, including in Ukraine and Georgia, has developed since the so-called Binary Options industry was outlawed in Israel in 2017. It has disproportionately relied on Australia and small handful of other countries for its growth.

The close-knit binary options industry once employed thousands of staff in Israel, many highly paid, operating a form of high-stakes unregulated trading akin to online gambling, much of it rigged. After 2017 it simply moved offshore and branched out. It now comprises businesses involved in affiliate marketing, lead generation and content creation, information technology, as well as payment service providers, and legal, recruitment, company formation and accounting firms, all with the common, if not explicitly stated, purpose of facilitating scams.

Call centres, each housing hundreds of operatives, run by Israeli-linked syndicates in Serbia, Cyprus, Bulgaria, Ukraine, Romania, Moldova, the Philippines and elsewhere operate dedicated teams on a shift pattern to coincide with the Australian time zone. The same modus operandi is used to target victims in Canada, which vies for the top spot with Australia as the Israeli scam syndicates' most favoured target.

These groups make heavy use of social media and social engineering to find, recruit and dupe victims. This includes mass advertising campaigns on Facebook and other platforms featuring fake celebrity endorsements of fraudulent crypto investment schemes, with campaigns tailored to each country's audience. They deploy sophisticated customer relationship management tools and techniques to track all their dealings with their "clients" and related businesses, and closely monitor staff and brand performance and every dollar moving in and out of their operations.

Several groups operate "educational" websites that purport to teach subscribers how to become day traders. In fact, although often a profitable online business in their own right, they are in fact just a tool to harvest leads for the syndicates' scam brands, part of a sophisticated marketing funnel.

Evidence obtained by IFW from inside just one of these groups shows it was recruiting approximately two to four thousand new Australian victims per month between 2020 and 2022.

IFW
GLOBAL

Most of these victims lost relatively small amounts, typically equivalent to about USD 250. A proportion were duped into losing their entire life savings, in some cases millions of dollars. The total amounts stolen from Australians amounted to several million dollars a month, with the total annual receipts by the group in the hundreds of millions.

There are smaller cells, many using British and American operatives to man their call centres, operating fake share trading, crypto and bond investment scams and targeting Australians from bases in the Philippines, Thailand, Cambodia, Malaysia, Dubai, and Indonesia, among other places. These groups cause significant damage but lack the industrial scale and sophistication of the Israeli syndicates.

The structural and operational failures that have allowed this industry to flourish are clearly visible to private sector specialist companies such as IFW, which is exposed to hundreds of cases every year. But they are just as obvious to frontline police and regulatory agency staff, who see the scale of the offending and the costs to the victims but find themselves powerless to act or not supported by managers.

Mid-ranking AFP officers have told IFW that the AFP "has no remit to investigate scams" and that its cybercrime unit focuses exclusively on "computer intrusion" type offences. At the same time, police detectives from state forces at District level frequently report that they have "tried to get the AFP interested with no result".

State police officers very commonly have a misconception shared by the Australian public and many scam victims: that since the offenders are overseas and the likely offences fall under Commonwealth law, the AFP will take the reports and deal with them. Unfortunately, this is not what happens.

(It is interesting to note that the AFP submission to this Inquiry focuses exclusively on its activities with respect to cyber-*dependent* crime.)

The few domestic state or federal prosecutions IFW is aware of that involve offending by organised overseas cyber-fraud syndicates relate to money laundering, not fraud.

Pursuit of the money laundering aspect of the offending is necessary but insufficient. Such prosecutions mostly target domestic offenders who are rarely able to provide useful evidence about the structure or operation of the syndicate or even the identity of people higher up. Such mules, patsies and facilitators are deliberately chosen and managed by the syndicates in such a way as to be dispensable.

The focus on the money laundering aspect also has the perverse effect of making the offending appear even more complex and daunting than it really is. Money laundering is dynamic and deliberately designed to be opaque. Laundering networks often operate separately from the scamming or overlap with it in complex ways. By contrast, the scamming – and thus from a legal perspective, the underlying fraud – is highly centralised.

IFW
GLOBAL

Legislative changes under which it is no longer necessary to establish the commission of a predicate offence to prosecute for money laundering give police more scope to go after syndicate members and offer the prospect of long sentences, but also provide another reason not to investigate the underlying fraud.

The Australian Securities and Investment Commission (ASIC), meanwhile, has focused almost entirely on local offenders even though virtually every serious organised fraud syndicate committing offences in Australia under the Acts administered by ASIC is based offshore, and ASIC has in some instances known exactly who was behind them.

Reliance on ASIC, or an expectation that it will act, is itself problematic. Casting the issue as primarily a regulatory one covered mostly by civil law gives an early victory to the scammers, as it helps obscure the fundamentally criminal nature and intent of their operations.

The overall approach just emboldens the scam syndicates and they have learned they can game the local regulatory system to their criminal advantage.

Overseas fraud syndicates involved in fake online trading, cryptocurrency, bond, and other types of scams have repeatedly set up ASIC-registered companies and hired local nominee shareholders and representatives in Australia to front their operations, knowing these disposable patsies will be the only ones in the firing line if ASIC or police investigate.

More alarmingly, IFW has evidence showing Israeli-run criminal syndicates have set up at least five cryptocurrency exchanges in Australia since 2020, registering companies with ASIC and obtaining digital currency exchange licences from AUSTRAC.

The sole purpose of these licensed exchanges has been to process and exfiltrate millions of dollars of scam proceeds stolen from Australian victims. Even consumers stumbling innocently on the exchanges have been victimised, with their details being used to generate cold calls from scams they had no idea were connected to the exchanges or their criminal owners.

In effect, there is **no** Australian agency with a proper remit to oversee investigations and prosecutions of these offenders or with an appetite to dismantle the networks responsible. This is in stark contrast to Australia's approach to other forms of serious organised crime, such as narcotics or illegal firearms importation or human trafficking.

Meanwhile, public policy has focused almost entirely on consumer education and domestic banks' responsibilities, and on measures to prevent, minimise or displace cyber-fraud rather than to prosecute or even understand it.

Australian media coverage, for its part, has focused on individual victims and domestic financial institutions and given almost no attention to the groups responsible for the offending, the geopolitical factors that have fostered their growth, or the structural issues and policy deficiencies that have made Australia such a juicy target.

IFW
GLOBAL

The federated nature of Australian law enforcement creates barriers and friction, but this does not explain or excuse these deficiencies. Some of Germany's 16 state agencies, for example, have been some of the most active and effective in criminally pursuing overseas scammers.

The same German agencies report, anecdotally, that rates of domestic complaint reporting have fallen in the wake of high-profile operations, which have included coordinated raids in multiple countries and the extradition of suspects, including from Israel.

The United States has also flexed its federated muscle to effect. When a court in Maryland jailed Israeli binary options scammer Lee Elbaz in 2019 and gave her a 22-year jail sentence, Israeli investment fraudsters had already had signs in their call centres for years warning operatives not to call US phone numbers. They knew the threat of prosecution and significant jail time was real.

2. International, federal, and jurisdictional coordination law enforcement mechanisms to investigate cybercrimes and share information related to emerging threats

At the time of writing IFW Global is working closely with law enforcement agencies in the US, Europe and across SE Asia as well as in Australia. Almost every IFW case involves multiple jurisdictions, and the firm is uniquely placed to observe the success or otherwise of interjurisdictional collaboration and information sharing.

There are two glaring issues in Australia that routinely confront IFW investigators, and frequently cause alarm at overseas agencies.

The first is a lack of information sharing and collaboration within Australia. This is among the factors that has made Australia a highly profitable and attractive target for scammers.

IFW has assembled several groups of clients where evidence has been obtained showing the same overseas syndicate was responsible for defrauding each member of the group. With each of these groups at least two Australian state police forces have opened investigations based on victim complaints.

For some of these groups there are separate investigations under way in all major states. But in almost every one of these cases, state police investigators had no idea there was a related investigation under way anywhere else in Australia until informed of this by IFW or one of its clients.

The second issue is a failure to share intelligence proactively with overseas agencies or engage with those agencies even when they send specific requests or provide intelligence or evidence to their Australian counterparts.

IFW often encounters bemusement about this among officials overseas. They cannot understand what they describe as a lack of interest in a form of offending that disproportionately targets Australians and has resulted in such significant monetary losses to the Australian economy.

3. Coordination efforts across law enforcement, non-government, and private sector organisations to respond to the conduct of cybercrimes and risks of cybercrime

Australian cyber-fraud victims who elect to report an offence usually make a complaint via the Cyber Incident Reporting System (CIRS). The report is then triaged. The most common response received by IFW's clients is that police can do nothing, but the information will contribute to intelligence gathering. Many clients report receiving no response at all.

Some cases are sent down to the victim's local police station. This is very often the last time these cases see the light of day.

IFW clients typically file complaints involving losses several times the threshold for serious fraud under Australian criminal law and not uncommonly involving more than AUD 1 million. But regardless of the size of the fraud, if scam cases are taken on at all, typically they are assigned to junior detectives – often sympathetic and keen but ill-equipped to deal with complex multijurisdictional cases.

The junior officer will sometimes try to get the case referred up to the state cybercrime unit. This rarely succeeds. If it does, the case is rarely connected to others in that jurisdiction or elsewhere.

The following example highlights these issues and is not exceptional:

In late 2023 an Australian state police cybercrime unit asked IFW for intelligence on a group of scams that the unit said it knew were connected, as well as contact details for overseas agencies that IFW had said were looking at the same offenders. IFW provided the unit the requested intelligence and contact details, along with details of separate but related prosecutions and investigations by two other state police forces and the Australian Federal Police.

IFW told the unit it would advise a client who had been defrauded in one of the scams and resided in the same state to file a CIRS report, so his evidence could be included in the various active investigations. The client then filed a detailed CIRS report. In response the client received an email stating:

> *Unfortunately, these types of investment scams are becoming very common, the perpetrators reside overseas and scam millions from people every day [...]*

IFW
GLOBAL

Thank you for bringing this incident to our attention. Unfortunately, due to the offenders being overseas and outside of Australia jurisdiction, your report will not proceed to investigation but will be filed for intelligence purposes only and closed.

If run at local state level, investigations often run into the sand at an early stage. The first hurdle is dealing with financial institutions, which increasingly include cryptocurrency exchanges.

Australian state police have improved in this area, but still lack adequate capability to trace cryptocurrency.

Crucially, there is also a lack of support for frontline officers wanting to engage with cryptocurrency exchanges once investigators, government or private, identify wallets that have received stolen funds, or to force disclosure of information identifying offenders when exchanges refuse to cooperate.

4. Emerging cybercrime threats and challenges affecting Australian entities and individuals, including the scale and scope of cybercrimes conducted in Australia or against Australians

The first point to make is that official and media reporting vastly underestimates the scale of victimisation and the resulting losses. This is only partly attributable to low reporting rates by victims.

In 2023 a European law enforcement agency provided to ASIC a database containing details of more than 30,000 individual Australian victims of a single Israeli fraud syndicate. The European agency has since identified a further 9,500 Australian victims of the same group. The total losses involved are estimated by the European agency to be several hundred million dollars.

This information is not publicly known and IFW is not aware that any domestic agency has taken steps to contact the Australian victims. Such an effort would have been noticed by IFW since it represents several dozen of the victims. By contrast, the European agency, which identified a few thousand victims in its own jurisdiction, has made efforts to contact each of them, to alert them and encourage them to file criminal complaints.

In another case, as a result of a single Australian prosecution of an alleged money launderer, police have identified more than 1,000 Australian victims of a different Israeli fraud syndicate. In that case the losses are estimated to be at least AUD 50 million.

In both cases IFW had alerted Australian authorities at least 12 months prior to official investigations commencing that a single overarching syndicate was responsible for multiple scam websites and that the scale of victimisation was very significant. Some of the offending took place after this.

IFW
GLOBAL

Cyber forensic analysis, transaction tracing and communications evidence obtained early on pointed to a network of scam websites and money laundering networks and a common single point of control. Further investigation proved up these connections and identified multiple entities and persons of interest, including in Australia.

The investigative techniques and resources used to make these findings were not particularly specialised. However, investigators were motivated from the outset to identify the "head of the snake" and not just chase its tail. This is not generally the approach taken by Australian law enforcement in relation to this type of offending.

Similar problems characterise the approach to preventing victimisation of Australians.

ASIC and the ACCC, like many overseas regulatory agencies, encourage reporting of scams and issue official warnings about particular websites or brands once it is established that they may be fraudulent.

The warnings have the benefit of encouraging victims to make official complaints and/or engage investigators, and they provide intelligence for investigators working on related cases. Unfortunately, they have little to no *preventive* effect since they are almost always published too late.

Scammers operate URLs until the weight of *unofficial* online complaints renders them unviable. They then simply rebrand the same website with a different name and URL. The more successful the scam, the longer it takes for victims to realise they have been duped and make complaints. As a result, these warnings about scam brands have no real *deterrent* effect either. By the time warnings are published, the scammers have moved on and found new victims with a rebranded website.

Since law enforcement agencies respond piecemeal to scams as they emerge instead of looking for their patterns and origins, the centralised structures from which the scams emanate are rarely identified.

Scammers even manipulate the unofficial complaints. Australian scam victims typically report that they "searched Google for any complaints or concerns" about the brand with which they have engaged and found none. This is because scammers are adept at Search Engine Optimisation – manipulating online search results, for example by publishing fake positive reviews and driving fake traffic to them, to ensure that only positive results appear on at least the first two pages of search results.

IFW has observed a very rapid rate of innovation and adaptation by fraud syndicates. In the last 12 to 24 months, they have begun using Artificial Intelligence tools to create fake online identities and content and deployed more complex and increasingly sophisticated cryptocurrency money laundering techniques including automation.

It must be noted that two key driving factors in the rate of cybercrime victimisation in Australia and other wealthy countries in recent years have not had anything to do with government or law enforcement.

IFW
GLOBAL

Rather, fluctuations in the price of bitcoin have fuelled fascination with purported crypto investment schemes, and COVID-related lockdowns have increased online activity generally.

Nevertheless, there is no reason for Australians to expect any significant decrease in the rate of victimisation from this type of crime or its economic costs in coming years unless Australia adopts better tailored and more proactive measures of prevention and detection, and most importantly, sends clear signals by its actions that the perpetrators face a real risk of criminal justice, no matter their location.

Recommendations

1. Australian government adopts policies to combat cybercrime that prioritise criminal investigation and collaboration with overseas agencies and are aimed at dismantling the criminal networks responsible. This should include a foreign policy component that addresses the responsibility held by nations hosting the fraud syndicates, which benefit from high-level corruption and/or regulatory weakness in many countries.

2. Australian law enforcement agencies establish and maintain intelligence sharing agreements with private sector firms and experts with relevant knowledge and expertise, to ensure agencies receive relevant, actionable, and timely intelligence and are empowered to interrogate it properly and collaborate effectively on investigations.

3. Cryptocurrency exchanges domiciled in Australia are obliged to operate under the same KYC and AML framework as domestic banks, including onshore storage of customer and transaction records.

4. CIRS data is analysed to identify emerging patterns and prevent or disrupt further offending at the earliest possible stage.

5. Measures are introduced to prevent the fraudulent use of VOIP telephone numbers that spoof Australian phone codes and measures encouraged internationally to block calls to Australians from numbers that spoof other locations, especially the UK.

Mark Solomons,
Senior Investigator
IFW Global Investigations Pty Ltd

Trusted for what is brought to light.

IFW

GLOBAL

Tel 1300 439 456

www.ifwglobal.com