GLOBAL COALITION TO FIGHT FINANCIAL CRIME

Financial Scams Report

An Assessment of Scams in East Asia - in Australia, Hong Kong & Singapore

By GCFFC Asia Chapter

June 2024

Financial Scams Report

An Assessment of Scams in Australia, Hong Kong SAR & Singapore

Executive Summary

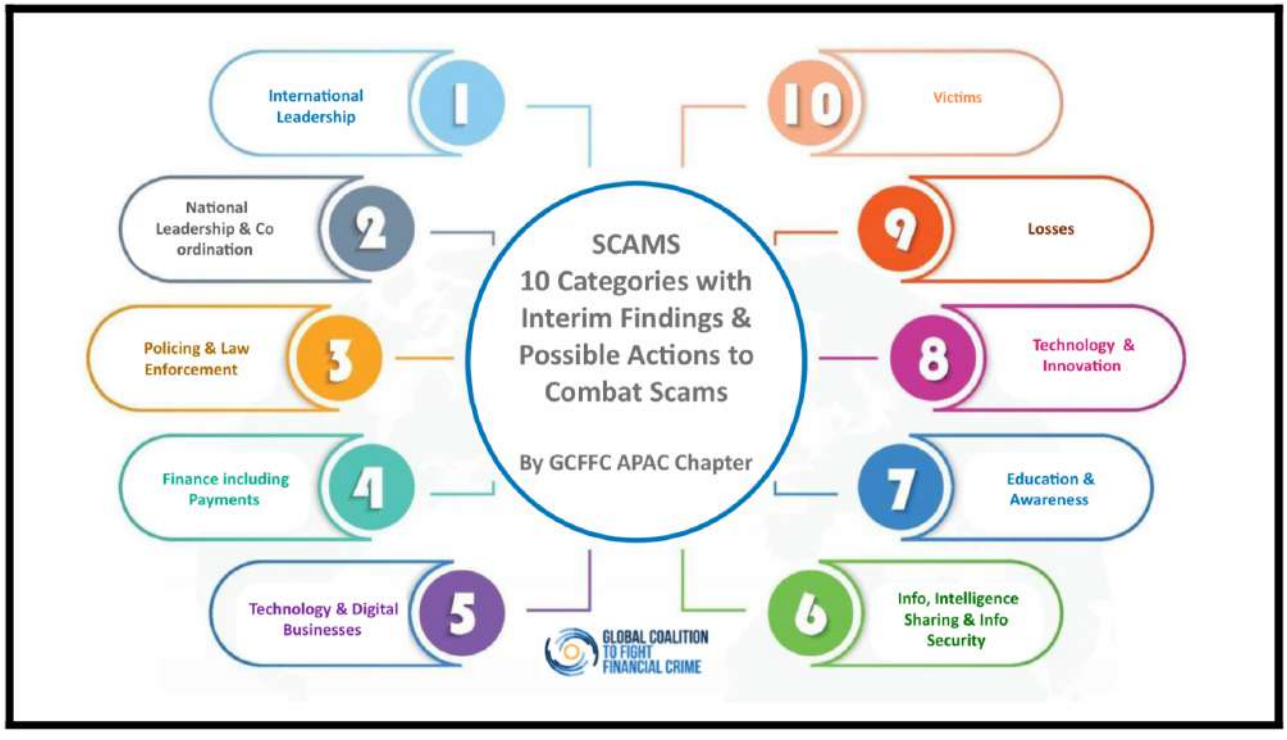
Whilst all countries are seeing an increasing level of scams, richer countries, for example, G7, EU & OECD member countries are reporting the most in terms of cases & losses. A few countries or jurisdictions are reporting sufficient information to be able to understand the threat well enough & appreciate the response. These include Australia, Hong Kong SAR & Singapore, which this report is focussed on, as well a handful of others, for example New Zealand, Taiwan, Canada, UK & USA.

There are more than 20 main types or variety of scam types identified in this report, with some hybrids & others involving additional forms of criminality, leading to financial losses, lifestyle changing consequences, & changes to life with 500,000 people estimated as modern slavery/human trafficking victims forced into criminality to support romance baiting and numerous suicides from scams such as sextortion.

Proceeds from reported losses from Australia, Hong Kong SAR and Singapore (as well as reported losses from other countries with reported losses, namely the UK, Canada & the USA) if extrapolated globally, generate estimates between US$50 Billion and US$177 Billion with a mid point estimate of **US$114 Billion,** which would make it the 64th largest country by GDP equivalent**.** Average losses per victim are estimated therefore at **US$12,000** and average losses per citizen at approximately **US$62**. Despite this, scam losses are widely acknowledged as being under reported.

Factors which make countries or jurisdictions more attractive targets, include those that are richer but also, more advanced in terms of digitalisation & connectivity, are able to offer digital remote banking & faster payments, with speedy remote opening of many new bank accounts, use of none cash including use of virtual currencies, significant online time being spent including on the internet & on social media & the availability & popularity of e-commerce, having languages spoken common to those of the scammers & of course a general limited awareness of enough citizens to scam types & tricks & how to defend themselves.

Based on the research carried out into Australia, Hong Kong SAR & Singapore and summarised in this paper, the GCFFC APAC Chapter believe a number of responses may have merit and is consulting on which of the focus areas and possible actions highlighted in this paper may make an important difference and could be supported going forward to improve the effectiveness in fighting scams. For more details, read this paper.



1. Introduction

The GCFFC APAC Chapter commissioned research into the scale, threat & response to financial scams, in the APAC region with a focus on Australia, Hong Kong SAR & Singapore. The research and the findings reveal similar scam threats which have been on the rise even prior to the Covid 19 pandemic. All 3 jurisdictions face similar challenges to upgrade responses to counter what is an ever evolving threat landscape. International responses are nascent, and international standards are not yet available and so responses can benefit from experiences, ideas and best practices that are working. These are summarised for Australia, Hong Kong SAR & Singapore in this paper. The findings from this GCFFC APAC Chapter review have generated comment and action on 10 key areas which the GCFFC is now consulting upon - See Section 10 below.

According to Interpol's Secretary General Juergen Stock in his assessment on global financial fraud published in March 2024[1], "*we are facing an epidemic in the growth of financial fraud, leading to individuals, often vulnerable people, & companies being defrauded on a massive and global scale. Changes in technology & the rapid increase in the scale & volume of organised crime has driven the creation of a range of new ways to defraud innocent people, business & even governments. With the development of AI and Cryptocurrencies, the situation is only going to get worse without urgent action. It is important that there are no safe havens for financial fraudsters to operate. We must close existing gaps & ensure information sharing between sectors & across borders is the norm, not the exception. We also need to encourage greater reporting of financial crime as well as invest in capacity building & training for law enforcement to develop a more effective & truly global response.*"

Scamming is probably the most commonly attempted and or experienced financial crime in the world. Scams take many forms but at their core involve an attempt to steal, ultimately for financial gain. This invariably includes dishonesty or deception, but under law is frequently covered by the offence of "fraud" and is a separate offence from "theft", with less elements in order to prove and or to convict. Whilst in many cases a "fraud" can be attempted and successfully carried out against a victim without the victims involvement or active knowledge "scams" usually involve in some way the victims unwitting participation.

In this paper we focus on what is often described as so called "authorised" scams, where the victim has been duped or tricked in some way so that the scammer can either steal identity or other highly valuable information such as bank account & or payment card details or is paid usually by victims giving access or information to the scammer or authorising the very payment, albeit under false pretences.

As more activities move online or are accessed through remote or digital channels, the availability, speed, cost & ease of use of new technologies provides significant benefits for all, but at the same time offers ever increasing opportunities for criminals to benefit, and to target so many more people than they would otherwise be able, and to successfully carry out all manner of traditional and evolving scams.

Scammers target weaknesses in design in technologies, and/or exploit poor online human hygiene & behaviours. Scammers also can't do this alone. They benefit from legitimate businesses, such as telco's, technology, internet, social media & higher risk e-commerce businesses to enable the scams and target victims' payment channels such as cards and accounts, to close out their scams. They also co opt others, for example money mules and use faster payments to speed up the transfer of funds and borderless banking to make it harder to track and trace scammed funds. The popularity of different types of scams will vary between countries, often depending upon the economic cycle, the awareness of scam risks & the controls & response levels by those businesses that enable scams and those that try to protect citizens from becoming victims and to help to investigate and recover losses.

In this paper the focus is on victims as private individuals & or businesses that are targeted by criminals through scams & not on other areas of fraud, such as public sector, insurance, securities or insider frauds.

2. The International Response to Scams

Scams have been around for millennia and continue to evolve, with yet no international agreement or common regional or international response. The rise of technology and digital businesses have propelled scams to become the fastest growing and most prevalent of financial crimes.

2.1 United Nations Convention on Cybercrime

There is no international convention on cybercrime, which means their is also no definition. The UN has been trying to agree one since 2019, but major disagreements have derailed what was already a complex process. A draft text had been produced after years of negotiations with nine chapters and over 60 articles. The concluding session for finalising the Convention took place between 29th January - 9th February 2024. Unfortunately, major differences meant that the session was suspended and is only expected to reconvene later this year. The main fundamental issue that divided opinion related to the scope of international cooperation in connection with cybercrime and the extent of human rights safeguards. Some governments opposed applying human rights protections to these cooperation efforts, whilst others felt if human rights safeguards were not applied the effect could be that some governments could end up facilitating prosecutions for political comment or dissent against an oppressive government. As the definition of "cybercrime" itself has become a contentious, the challenge is how to reconcile one sides opinion that the focus should be to address only computer-related offences, like attacks on computer data or systems, whilst for others it has to be broader and should also apply to a larger number of crimes which could include forms of online expression[2].

2.2 Bank for International Settlements in Basel Switzerland

According to the BIS in their Discussion paper, Digital fraud and banking: supervisory and financial stability implications, dated November 2023, and issued for comment to 16 February 2024[3], the BIS reviewed the trade-off between digitalisation benefits and digital fraud risks, but rather than focus on the risks to customers the BIS was more concerned with the risks to banks themselves, highlighting financial stability, through potential reimbursement losses and reputation risks[4], which were of concern for supervisors.

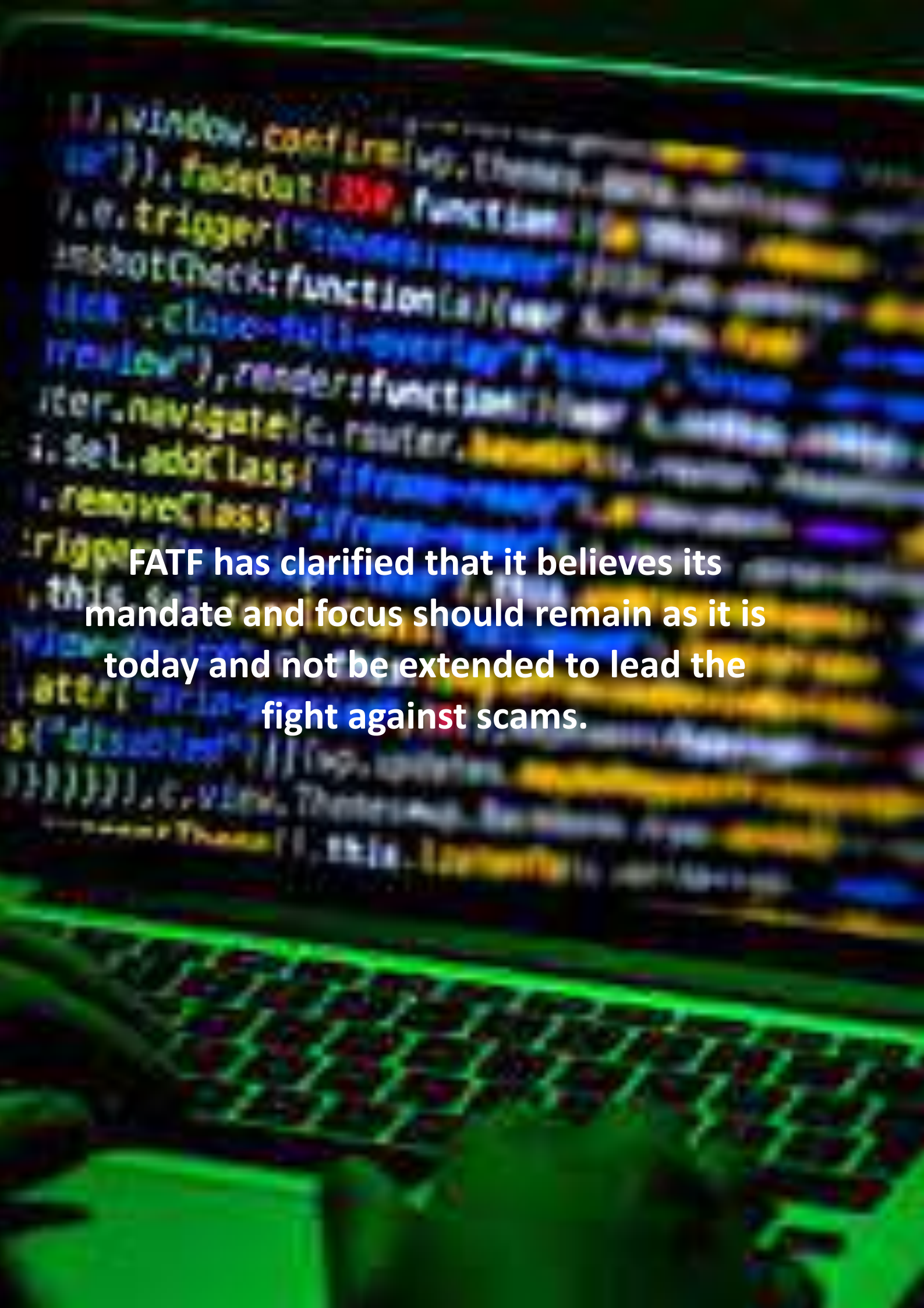
2.3 Financial Action Task Force (FATF) on Money Laundering (ML) and Terrorist Financing (TF)

Fraud which includes "scams" is one of the FATF's' 22 predicate crimes to ML, but in many ways it is unique, in that it is not the result of a criminal bargain based on the supply and demand of an illegal product or a service, where illegal proceeds are generated & then laundered to hide the monies connected to the crime. With fraud (& scams) it is much more like theft, with the assets being stolen usually money or it's equivalent & then quickly transferred, often beyond the ability of the victim & or law enforcement to recover the funds. Whilst FATF has recognised the growing threat from scams, it has focussed on the laundering of the proceeds of "cyber enabled fraud", due to its mandate to follow the money & not on the crime itself, leaving a hole in the international response. See for example FATF's recent excellent Illicit Financial Flows from Cyber Enabled Fraud Report 2023[5], which focusses on the money flows. FATF has clarified that it believes its mandate & focus should remain as it is today & not be extended to lead the fight against scams.

2.4 Other Initiatives

A number of international and or regional initiatives have started to bring countries and jurisdictions together to discuss scams. For example.

- A Regional Anti-Scam Conference was held in Singapore in 2023[6], representing 15 countries.
- The UK hosted an international ministerial level summit on 12th March 2024[7] which including G7 countries plus, Australia, South Korea, Singapore & New Zealand which culminated in a call to arms communique[8]. An Agreement was reached to drive forward an international partnership to do much more to tackle fraud online.



FATF has clarified that it believes its mandate and focus should remain as it is today and not be extended to lead the fight against scams.

3. Harms from Scams (not just Financial Losses)

3.1 Harms

Scams are to some a cost of being online and for others of doing business. Whilst losses as a percentage of GDP and per citizen are relatively small, loss amounts per victim can be substantial and in terms of impacts on victims can be lifestyle and life changing. Don't be fooled, scams cause harm in many ways, whilst financial loss can cause great pain, severely impact self-esteem and peoples lives & lifestyles, harms don't just come in terms of dollars & cents either. For more on the impact and harms from scams see below:

- Proceeds from scams figures are hard to come by. Actual reported losses from victims are a good source but don't show the whole picture. For example, the Australian Bureau of Statistics (ABS) Personal Fraud data showed that in the 2022–23 financial year, 2.5% of Australians (514,300) experienced a scam and that 31%[9] of victims had not reported their experience.. It may be likely that many of those who did not report incurred only a small or no direct financial loss and consequently any under reporting does not mean reported losses would be 31% higher if those people had reported, but it does mean that reported losses are likely underestimated.

- Victims can often suffer from mental health problems, feel ashamed & or blame themselves. In a recent UK study[10], 55% of scam victims reported to have struggled with their mental health, 48% had experienced depression, 51% had low self-confidence and self-esteem & 26% experienced physical changes as a direct result of losing money, including losing or gaining weight, experiencing headaches and suffering from panic attacks, whilst 69% had experienced sleep problems.

- Victims can be re victimised as scammers pass on details from successful scams to other scammers to target the victim once more using much of the same information about the victim including their identity, contact & behaviours.

- Victims themselves can become involved in criminality. For example, once duped in a romance scam, victims have been asked to act as money mules, so that payments can be made through their bank accounts, to take out loans for the scammer and to misrepresent statements to the bank or finance company. Victims have also been forced into prostitution by romance scammers.

- Successful scams at scale can undermine confidence in financial services as well as online e commerce.

- The proceeds from successful scams for organised criminal gangs can also support poly criminality, with organised crime gangs also involved in activities such as drugs trafficking, human trafficking, arms trafficking & people smuggling. It can also support corruption used to facilitate and protect scammers.

- Harms from scams such as sextortion include self harm and even suicide. In the USA, according to the FBI and Homeland Security, from October 2021 to March 2023, there were over 13,000 reports of minors sextorted, primarily boys, which led to 20 suicides[11].

- Romance Baiting/Pig Butchering involves fattening up a victim of a romance scam to make them a victim of an investment scam. Those scamming the victims are themselves very often victims of job scams, lured into foreign countries & kidnapped and kept in compounds and forced into criminality to generate monthly proceeds from romance & investment scams. Conservative estimates of proceeds of crime generated from forced criminality from "Romance Baiting/Pig Butchering" scams, have produced figures of at least **US$25 Billion** per year[12]. More recent estimates suggest half a million "modern day slaves" have been lured into compounds not just in South East Asia, though this is the main region of operations of organised scam gangs. Estimates of those held and forced into scam centres include those in Cambodia (100,000) and Myanmar (120,000), but also in Laos (85,000), China (30,000), Dubai, UAE (20,000), Philippines (15,000) & Other Countries (130,000)[13]. With estimates for average daily proceeds generated at **US$350** per day, this would generate overall scam proceeds estimated at **US$64 billion** a year.

3.2 Reported Financial Losses

There are only a few countries that provide publicly available information on reported scam losses and cases, and do this regularly, for example at least annually. Based on reporting from 6 jurisdictions including those assessed in APAC (Australia, Hong Kong SAR and Singapore) and from Canada, the UK and USA, it is possible to aggregate reported losses and to estimate possible global estimates based on reports from these 6 jurisdictions, which represent approximately a third of global GDP. Based on reported loss figures, (recognising that a substantial amount of scam losses may also be unreported):

- Proceeds/Losses from reported scams from the 6 countries or jurisdictions which represent 31.5% of Global GDP, amounted to **US$17.8 Billion**

- If this was applied and extended to the rest of the world, that would generate estimates of approximately **US$55 Billion.** Estimates from just pig butchering scams are estimated at **US$64 Billion** - see above.

- Of the 6 jurisdictions there was significant variations in losses, both in terms of losses per victim, losses per GDP and losses per citizen (based on population size). Based on losses per GDP these ranged from 0.03% (Canada) to 0.3% (Hong Kong). Applying these amounts would generate estimates for proceeds/ losses at between **US$32.1** and **US$321 Billion** globally, with a mid point at **US$177 billion**

- Based on estimates of US$55 Billion and US$177 Billion a mid point estimate would be **US$119 Billion**

- Based on losses per victim these range from US$502 in the (UK) to US$29,000 (Hong Kong) with an average of approximately **US$12,000** per victim and based on losses per citizen, with a range of US$11 (Canada) to US$155 (Hong Kong) and an average of approximately **US$62**.

Comparative Analysis
Proceeds of Crime/Losses by Value
Scams in Australia Canada Hong Kong SAR Singapore UK & USA

Proceeds/Losses			
	Australia	Canada	Hong Kong SAR
Proceeds/Losses from 2023	AU$2.74 Billion	C$569 Million	HK$9 Billion
Change from 2022	(-13% from 2022)	(+ from C$530M in 2022)	(+ from HK$4.8Billion in 2022)
US$ Proceeds/Losses 2023	US$1.88 Billion	US$415 Million	US$1.16 Billion
Average US$ per victim	US$3,128 (AU$4,565)	US$13,551 (C$18,480)	US$29,000 (HK$226,000)
Average US$ per person	US$72 (AU$107)	US$11 (C$15)	US$155 (HK$1,200)
As %age of Country GDP	0.1% (US$1.7 Trillion)	0.03% (US$2.1T)	0.3% (US$360 Billion 2022)
Main Scams by Losses 2023	INV, RA, BEC, ROM, PHISH	INV,ROM,PHI,SERV,EXT	INV, IMPER, JOB, FFR, ECOM
Proceeds/Losses			
	Singapore	United Kingdom	United States
Proceeds/Losses from 2023	S$651.8 M	£1.17 Billion	US$12.3 Billion
Change from 2022	(-1.3% from 2022)	(-4% from 2022)	(+14% from 2022)
US$ Proceeds/Losses 2023	US$482 Million	US$1.49 Billion	US$10.3 Billion
Average US$ per victim	US$10,514 (S$14,189)	US$502 (£395)	US$14,927
Average US$ per person	US$83 (S$112)	US$22 (£17)	US$31
As %age of Country GDP	0.1% (US$$467 Billion 2022)	0.05% (US$3T)	0.04% (US$25.44T)
Main Scams by Losses 2023	INV, JOB, IMPER, ROM, MAL	IMPER,INV,ECOM,ROM,BEC	INV/IMPER

Global reported losses from scams could be between US$55 Billion and US$177 Billion - with a mid point at US$119 Billion.

Global average losses per victim estimated at US$12,000 and average losses per citizen at approximately US$62.

Note: Scam losses are widely acknowledged as being under reported.

4. Main Scam Types

There are many scam types, which come in many forms & variations but at their heart all require deception. Deception can be very basic, “click on this link”, from an unknown messenger, to click on a link on a new fake website, to “fake friends” or “it’s me” scams, to more of a complex set up, with “impersonation”, from government, bank, telco & “romance”, “investment” & “job” scams falling into these categories.

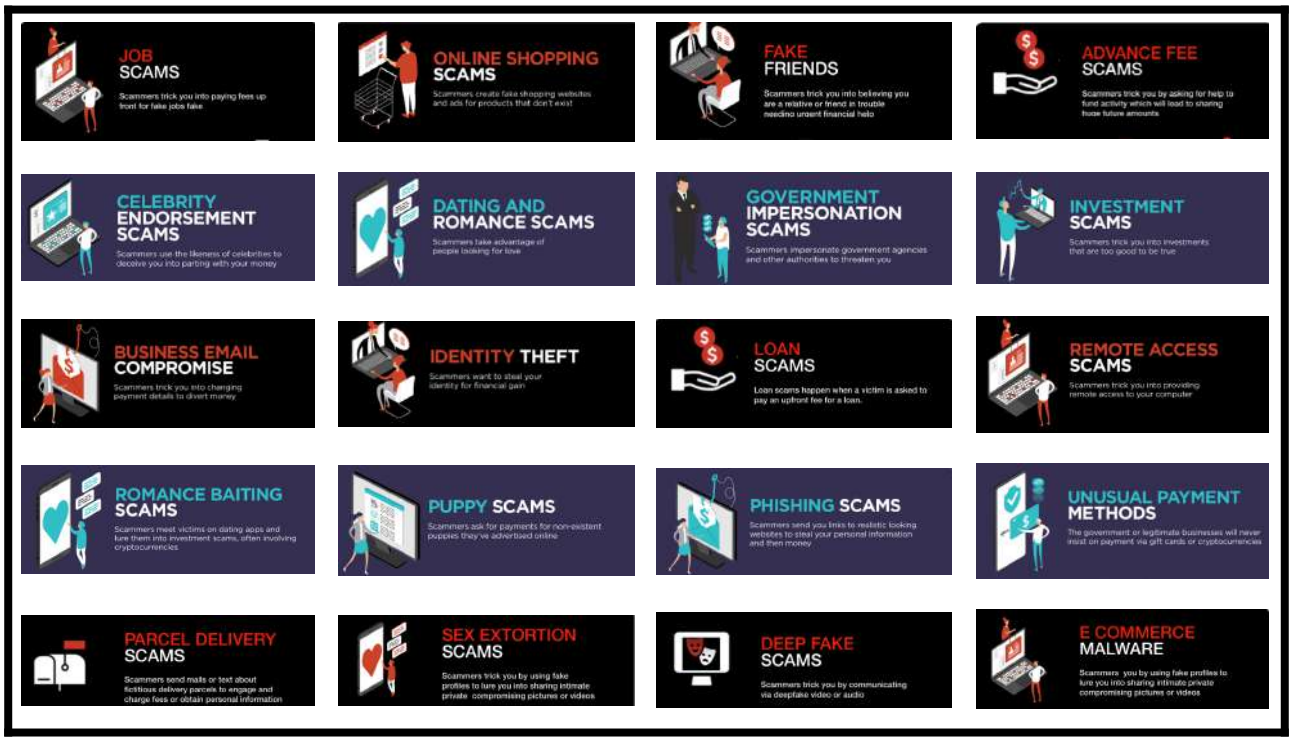
They can also be very sophisticated. For example, a recent “business e mail compromise” type scam with a modern twist was reported by the Hong Kong Police in January 2024. A finance department employee of a UK Headquartered engineering company, Arup, but based in HK transferred HK$200 Million (US$25 Million) to a 3rd party - a scammer. He had already received a suspicious email purportedly from the Company’s HQ in London requesting he carry out secret urgent transactions. It was only when he joined an online meeting which included the CFO who told him to make the payments that he put his original concerns out of his mind. Unfortunately all those others in the meeting were very realistic deepfake images and voices[14].

Scams target individuals & businesses, with the success rate greater in terms of numbers for scams against individuals. However the most successful scams in terms of proceeds come from successful scams against businesses which are higher value targets, with the Arup scam case above a prime example.

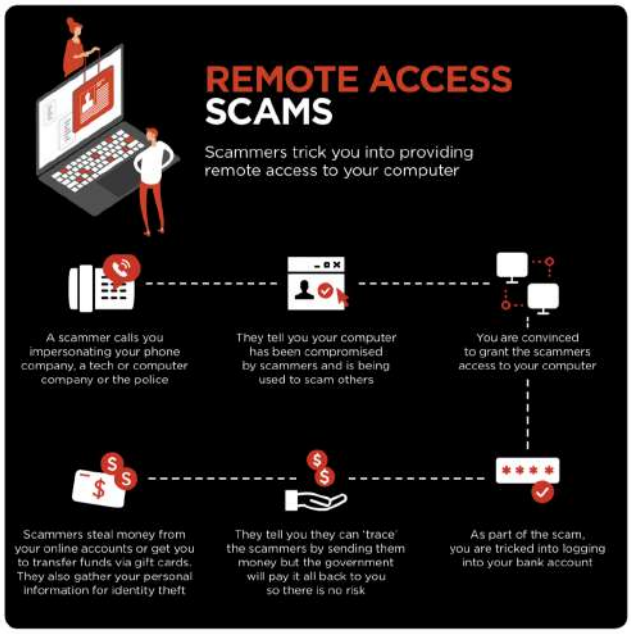
Scams were prevalent before the COVID pandemic, but this period was important & has accelerated activity & behaviours that benefit the scammers. Firstly with lockdowns the norm, it forced many criminals to adapt & turn to scamming from other criminal activity or even from other legitimate jobs. Secondly, the increase in remote working & the rise in people spending more time online, being more easily contactable by phone, text, email, on the internet & via social media, increased the target audience for scammers immeasurably. Thirdly the scammers got creative. Scams like job, romance & Investment scams have been combined to create “romance baiting/pig butchering” & romance & extortion scams have been combined to produce sextortion scams.

4.1 Top 20 Scam Types

Some scams are more popular & successful than others. The following 20 scams, include also phishing, e commerce malware, ID theft & unusual payment methods which are not technically scams but are related to & or preparatory to or related to successful scams & so have also been included as main scam types.



4.2 Job Scams: Job scams often start on online platforms, through fake job adverts. A prospective employee is ultimately deceived into paying a fee to get hired, or pays other fees upfront for training or equipment before starting. Variations may include suspicious or too-good-to-be-true job offers, or job applications that are targeted to collect unnecessary information (like social security numbers or bank details, etc). For job scams related to “romance baiting” or “pig butchering” see below.



4.3 Remote Access Scams: Scammers trick the victim into providing remote access to their computer or device. The victim may be contacted by a scammer, claiming that they have spotted a problem with the victims computer and offer to take remote control to fix it. The scammer may even claim to be calling from a bank and need to help with a problem with an account. To fix it, they ask the victim to give them remote access to the computer – they’ll explain how to do this – and then if they are after banking details, ask to log in to an online banking app, and ask for personal details, passcodes and card information, which they’ll then use to access the account. New malicious malware can also achieve the same thing. For more see E Commerce Malware below.

4.4 Online Shopping/E Commerce Scams: These involve scammers who pretend to be legitimate online sellers, either with a fake website or a fake advertisement on a genuine retailer site. These also include Payee/Payment Scams where the victim pays for goods (e.g. cars, technology, holiday rentals & concert tickets), that are never shipped & the seller then usually disappears usually from online platforms or social media. While most online sellers are legitimate, unfortunately scammers can use the anonymous nature of the internet to scam unsuspecting shoppers. Scammers use the latest technology to set up fake retailer websites that look like genuine online retail stores. They may use sophisticated designs and layouts, possibly stolen logos, and even a domain name similar to an authentic retailer. Many of these websites offer luxury items such as popular brands of clothing, jewellery and electronics at very low prices. Sometimes goods are delivered. More likely than not, though any delivered goods will be a "knockoff" items. Mostly no deliveries will be made. Scammers also use social media to advertise fake websites.

4.5 Advance Fee Scams: These scams are one of the oldest and most well known yet the volume of attempts still snares some victims. In this scam type the scammer tries to convince their victim to pay a fee which they claim would result in the release of a much larger payment or high value goods, which are also called 419 scams named after the section in Nigeria's penal code relevant to these types of crimes.

4.6 Investment Scams: Scammers seek to benefit by preying on people's financial insecurities or fear of missing out on high returns. Previously criminals typically used cold calling to target their victims, however indications are that now they are using sophisticated techniques to commit this form of scam, including abusing Search Engine Optimisation & creating fake comparison websites to drive customers to cloned scam websites. Customers will often be instructed to complete online forms to register their interest, before receiving a call from someone impersonating a genuine investment firm or broker. Scammers are also using social media and digital messaging services to promote bogus investment opportunities, including in forex trading & cryptocurrency – the latter fuelled by the demand for virtual currencies such as Bitcoin.

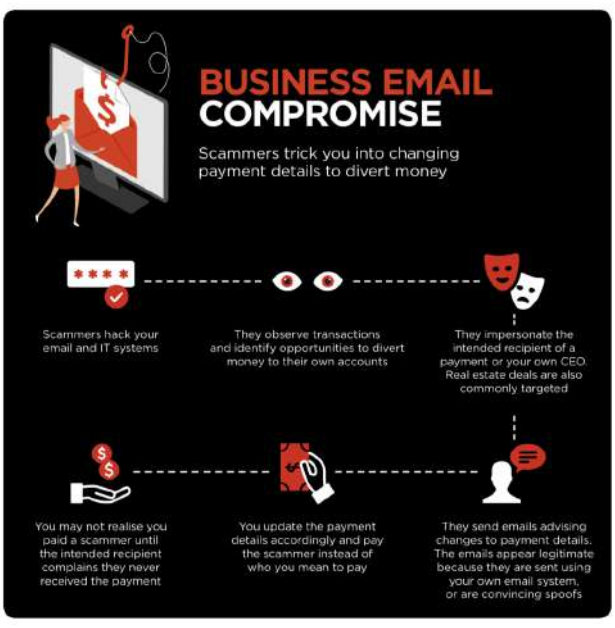
4.7 Impersonation Scams: These scam types have seen big increases and scammers have turned to mass scam texts, phone calls and emails impersonating trusted organisations such as Government departments, including tax, police and health or welfare and also those in the private sector such as banks, utilities &, telco providers in a bid to scam consumers to trick people into giving away their personal and financial details. For a more recent emerging popular related scam see parcel delivery scams below.

4.8 Dating & Romance Scams: The Covid pandemic is also thought to have helped to drive up cases of romance scams, as social distancing restrictions led to a significant increase in online dating and provided an opportunity for criminals to take advantage of this. Scammers create fake online or dating profiles, then make contact and try to gain trust and build an online relationship. They are usually based in a foreign

country and cannot meet, though promise to do so one day. At some stage, the scammer will explain that they have problems and need financial help and ask for money.

4.9 Celebrity Endorsement Scams: The rise of celebrity and influencers with significant followings make them candidates for endorsements. Celebrities and Influences can be used as part of a deception campaign, and to support for example investment or online shopping scams, but scammers may also use fake celebrity and influencer endorsements too.

4.10 Business E Mail Compromise (BEC)/CEO/Invoice Misdirection Scams: In this scam, the scammer targets businesses with the scammer trying to impersonate the CEO or other senior business leader, to direct payments for fictitious activity or transactions. Alternatively, an invoice is intercepted and or changed to redirect legitimate payments to the scammers accounts. A recent case involved deep fakes, see above and below.



4.11 Fake Friend Scams: A derivative of the impersonation scam is the “fake friend” or “Guess who” or “it’s me” scam. In this scam, grandparents or other family members or friends are asked for urgent financial help

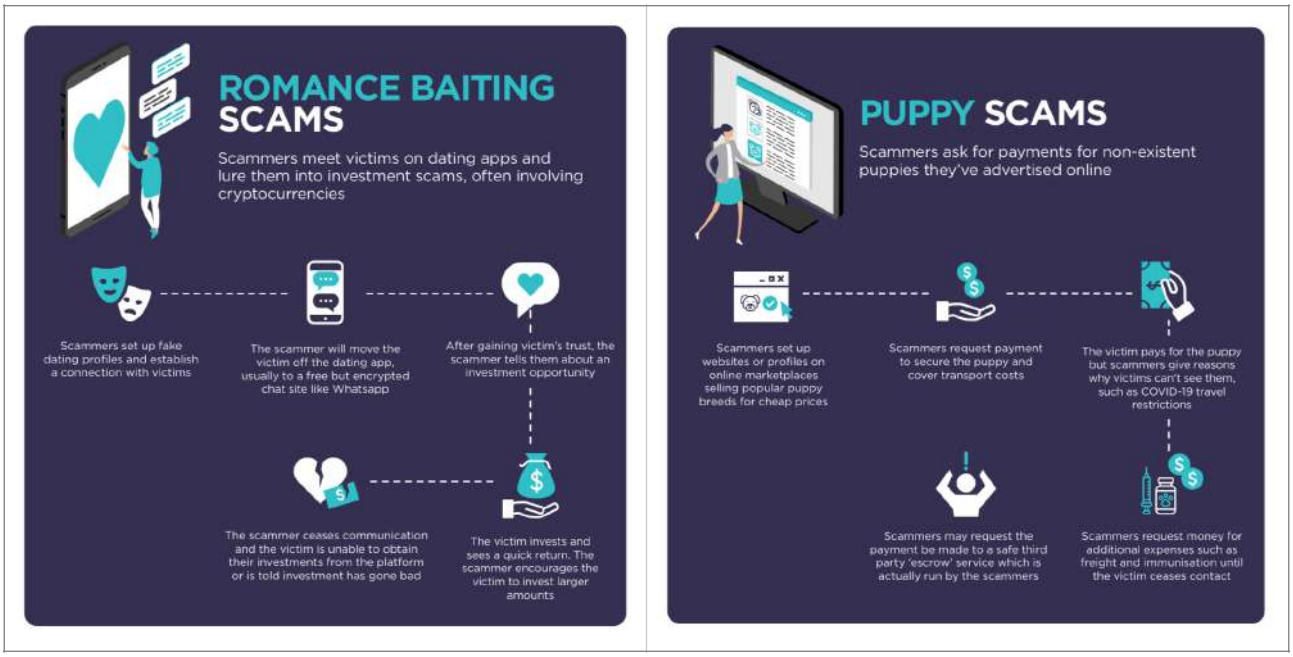
from those they may not have heard from in a long time, often with please don't tell mum or dad. An adaptation is a mail or other communication where family or friends receive requests from texts or WhatsApp messages from other phones they have borrowed claiming to be from their child who has lost their phone, and again need urgent financial help. A new variant is that scammers would send the victims malicious links and ask victims to help them in simple tasks such as making a purchase or making a restaurant reservation or tracking a missing phone. For more on these malicious links see Phishing & E-commerce Malware Scams below.

4.12 Identity Theft: Identity theft involves stealing personal details which may then be used by scammers to commit fraud. As a result cases of identity theft are often a pre-cursor to a scam. but it is often not considered a recordable crime. Identity fraud can be described as the use of that stolen identity in criminal activity to obtain goods or services by deception. Scammers can use 3rd party identity details to open bank accounts, obtain credit cards, loans and state benefits, order goods in that name, take over bank accounts, take out mobile phone contracts, obtain genuine documents such as passports & driving licences. Scams targeting identity theft can lead to additional scams being carried out using the victims credentials which can have a direct impact on personal finances and could also make it difficult to obtain future loans, credit cards or a mortgage.

4.13 Loan Scams: Targets for loan scams are borrowers who are duped into applying for fake loans but are then faced with paying up front fees as a pre condition to obtaining the loan. This scam is often targeted at those that have poor credit histories and can't access traditional loans and are feeling quite desperate, which is then used by the scammers to dupe them into making upfront payments. Once a payment is made, additional payments may be demanded. The scammers do not provide the loan funds to the victim, however much is paid upfront.

4.14 Romance Baiting/Pig Butchering Scams: This is not a new scam but it is growing fast. It is referred to as "pig butchering" or "sha zhu pan" in Chinese, which refers to the process of scammers "fattening" their victims by slowly building their trust before killing the pig, or taking the victims money. It became widely reported around 2019 as a scam that was targeting men in China, but the criminals have since widened their net. Pig butchering is a sophisticated new twist that combines a romance scam with an investment fraud and involves a time-tested, heavily scripted, and contact intensive process to "fatten" up the victim before "slaughter". This scam is predominately executed by scammers who mine dating apps and social media sites in search of potential victims. It involves creating a fake profile used to reach out to potential victims often through social media, WhatsApp, Tinder or other dating sites, and even using random texts, masquerading as an incorrect number or an old acquaintance. The goal is to initiate contact with a potential victim, attempting to be their "new friend" or "lover". The new friend creates reasons to continue a

conversation, which leads to multiple calls. While building trust with the victim, they slowly introduce the idea of making a business investment using cryptocurrency or foreign exchange. The victims are encouraged to invest small amounts in the beginning and the scammer will show the victim that they have made a modest gain on the investment. They may even allow the victim to withdraw money once or twice to convince them the process is legitimate. The victim is then persuaded to invest larger amounts on the fake platform, sometimes hundreds of thousands of US dollars. Eventually the scammer vanishes, taking all the money with them, resulting in significant losses for the victim. Pig Butchering involves human trafficking. In order to carry out the scam, the criminals have lured thousands of people into "scam sweatshops" often run by Chinese or other South East Asian criminal syndicates, many of them in the Cambodian coastal city of Sihanoukville, but also elsewhere in South East Asia. Enticed by fake job ads, the workers are coerced into defrauding people around the world. If they resist, they can face beatings, food deprivation or electric shocks. In a statement in August 2022, the UN's special rapporteur on human rights in Cambodia, Vitit Munterbhorn, described conditions endured as a "*living hell*", also stating that "*If the scammer refuses to comply with the orders, the person might be tortured or locked in various compounds surrounded by barbed wire and iron fencing to prevent escape*[15]*".*



4.15 Puppy Scams: Puppy scams are the most popular of pet scams, which are used to attract victims by offering a cute puppy or other pet for sale. These are similar in effect to Online/E Commerce scams using pets and in particular puppies. For more on Online/E Commerce scams see above.

4.16 Phishing: This scam is the most common of all scam types by cases, albeit of itself it is more a preparatory act towards a scam being used to capture information including the theft of information from the victim. There are different and or related types of phishing related scams, for example:

- **Email Phishing:** The most common type of phishing attack. Cyber criminals impersonate individuals, companies or charities in an email, directing potential victims to click a link and enter personal information or pay for something. Any data entered can be seen by the cyber criminals, including passwords.

- **Spear Phishing:** A targeted form of email phishing, where personal information is used to craft more genuine-sounding messages and usually targeting a specific victim.

- **Whaling:** A form of spear phishing, whaling is where cyber criminals target senior executives and high-ranking managers. These messages convey a sense of urgency, usually to transfer funds quickly.

- **Smishing:** Cyber criminals send text messages posing as an individual, company or charity. These messages work much the same way as email phishing.

- **Vishing:** Vishing or voice phishing is used by scammers who call their targets or leave voice messages and attempt to get victims to give information, such as account credentials or credit card details, over the phone.

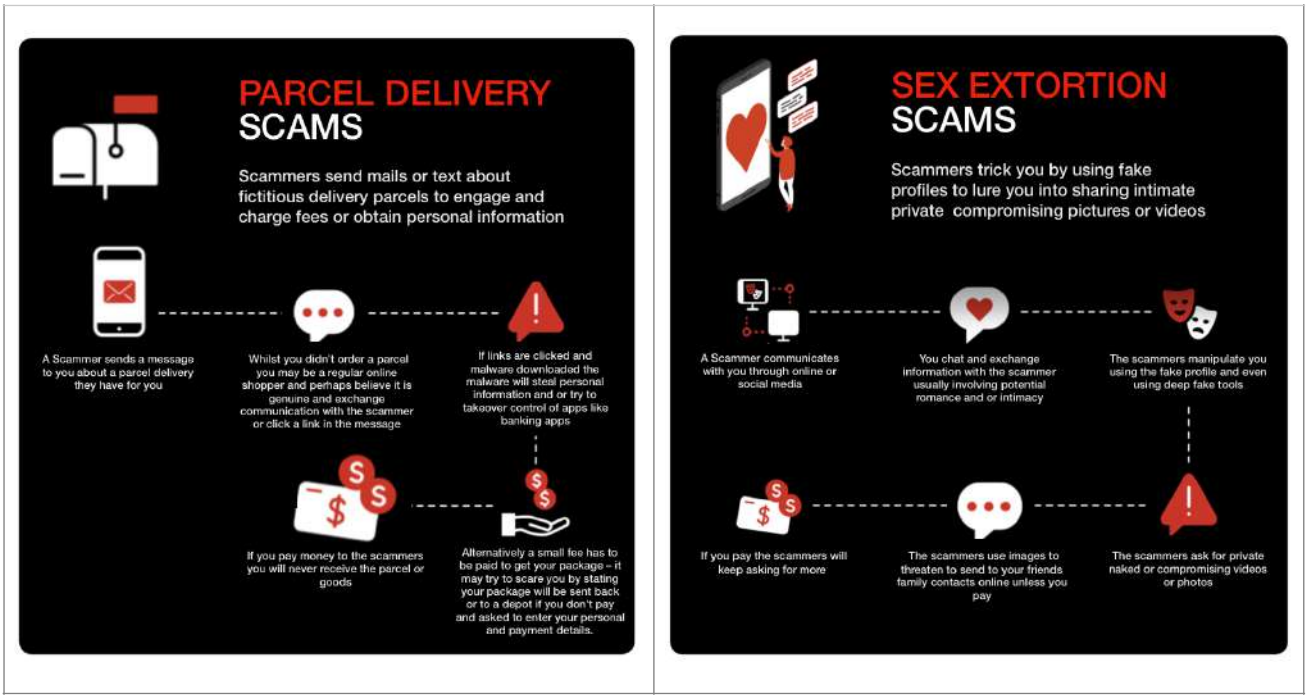
- **Angler Phishing:** Angler Phishing is named after the "anglerfish" whose most distinctive feature, worn only by females, is a piece of dorsal spine that protrudes above their mouths like a fishing pole—hence their name. Tipped with a lure of luminous flesh this built-in rod baits prey close enough to be snatched. Their mouths are so big and their bodies so pliable, they can actually swallow prey up to twice their own size. This form of phishing occurs in social media and online often with scammers targeting those that have complained about an online services and presenting themselves as customer service agents of the company complained about in order to obtain information.

A new variation and emerging threat scam are Malware Enabled Scams. These scams involve the use of malicious software to gain unauthorised access to a user's personal information or to deceive the user into making financial transactions benefiting the scammer. See for example E Commerce Malware below.

4.17 Unusual Payment Methods: Whilst not a scam in the traditional sense, scams are often associated with unusual payment methods. These include scammers asking for payment in gift cards. I Tunes or google play cards, via mobile transfer agents or in cryptocurrency. These payments are often less traceable.

4.18 Parcel Delivery Scams: Scammers attempt to trick victims into downloading malicious software (known as malware) by sending scam "missed parcel" SMS text messages or email or WhatsApp messages. Around holiday, festive, religious periods, this type of scam is even more prevalent, as many people may be expecting deliveries. The scam SMS messages contain links to what appear to be 'official' delivery/parcel-tracking apps, which the victim is encouraged to install. The 'app' is in fact a type of malware. If installed, this malware can steal banking details, passwords, and other sensitive information. The malware may also attempt to access contact lists and send scam SMS messages to contact numbers as well, helping the malware to spread across the world. Alternatively the message may state that a failed delivery of a package at the address was missed and a small fee is payable to arrange redelivery. The scammers then urge the victim to click a 'tracking link' to update delivery or payment preferences. Some of these links will direct victims to websites that prompt the entry of personal information or may inform that a phone is infected with malware and anti-virus software should be downloaded. Scammers may also direct a victim to a scam phone line where the operator will attempt to verify account details and credit card numbers, or even try to make the victim pay a charge for releasing a parcel or pay a fake customs fee.

4.19 Sex Extortion (Sextortion) Scams: Extortion, and especially "sextortion" emails and messages are becoming more frequent, and they can be extremely alarming when received. Such emails work by using threats to extort money, evoking intense fear. This type of correspondence comes in many guises and features various elements, but essentially, they work in the same way. These activities can refer to real-life experience such as cheating on a partner or online behaviours such as visiting porn sites, or from sharing nude or compromising pictures, videos or other potentially embarrassing information. They are often called sextortion scams where there is an element of sexual behaviour to them, something which is highlighted by scammers as undesirable and shameful. They usually threaten to expose the victim's shameful activities to colleagues, friends, and family. Scammers then ask for payment to keep this a secret. Although sextortion scams are not new, they have evolved drastically in the past few years. Historically, victims of such scams were usually young women, typically targeted by someone they dated in real life or met online and who was in possession of private or sexual images of them. More recently, criminals started targeting teens and children and coercing them to send explicit images of themselves, which are traded by criminals. Additionally, there are also sextortion emails sent to private individuals, who have never had any prior contact with their perpetrator. Most ask for payment in cryptocurrency. This is a convenient payment option for cybercriminals because virtual currency, has little or no legal effective regulation across many different countries and makes it an attractive choice for moving illicit funds.



4.20 Deep Fake Scams: A deepfake is a type of digital content – usually video or audio – that has been generated using artificial intelligence and mimics a person's likeness or voice. And they are becoming increasingly hard to tell apart from the real thing. Today's advanced machine learning algorithms can manipulate images, audio and videos in a way that makes the resulting deepfakes convincingly realistic. The technology holds promise for various uses, such as creating digital doubles in films or providing customised support to students. But it is also being used and is likely to grow substantially in the armoury of scammers. Deep fake technology can create the illusion of someone saying or doing something but is fake, and can support investment, romance, fake friend and other scams. Deepfakes of children's voices have also been used for scam kidnappings.

4.21 E Commerce Malware: Scammers are introducing malicious links in e commerce sites, but also include them in phishing attacks. These malicious links will lead victims to either phishing sites and/or the download of an Android Package Kit (APK) file, an application (app) created for Android's operating system. After keying their banking credentials or card details at phishing sites provided by the scammers to make payment, victims will then discover unauthorised transactions from their bank accounts or incur charges to their bank cards. Once victims download and install the app containing malware, the malware will allow scammers to access the victims' devices remotely and steal passwords stored in the devices. Victims may

also be directed within the app to fake bank application login sites to key in their banking credentials to make payment within the app. The malware with keylogging capabilities would then capture the credentials keyed by the victims in the fake banking sites and send it to the scammers. Unknown to the victims, the scammers would access the victims' banking accounts to perform unauthorised transactions. There are dangers in downloading apps from third-party or dubious sites that can lead to malware being installed on victims' mobile phones, computers, and other devices. Scammers will trick victims into installing malware-infected apps that are outside the app store. Members of the public are advised not to download any suspicious APK files on their devices as they may contain phishing malware.

4.22 Emerging Scams

The main emerging threats and threats increasingly of concern include, E Commerce Malware, Deep Fakes, Romance Baiting/Pig Butchering & E Commerce/Online Scams.

Two of the biggest recent scams have revolved around fake tickets for major events, including fake Olympics and Taylor Swift tickets, as well as other online/e commerce shopping. According to the FT, "*Most ticket scams start on social media, with sellers pretending to re-sell tickets for events. Tickets may never be received or might sometimes appear real, but not allow customers to enter venues at the door. More sophisticated fraudsters also create fake ticketing websites to harvest customers' data. Scammers will typically request that victims send money via a bank transfer. This makes it harder, in the absence of a chargeback mechanism, for them to retrieve their money. Most individual scams are worth more than £100, according to Santander UK. With concert and sporting events tickets, however, amounts can reach many times that as scammers take advantage of the hype and "fear of missing out" around events that can sell out within minutes. In the U.K., one Bank stated that Taylor Swift fans have lost an average of £332 each in ticket scams, with some victims paying more than £1,000. The bank said scammers selling fake Taylor Swift tickets had targeted customers aged 25 to 34, and that 90% had done so via Facebook*"[16].

A HK finance department employee of a UK headquartered engineering company, Arup, paid HK$200 Million (US$25 Million) via 15 transactions to a scammer.

He had already received a suspicious email purportedly from the Company's HQ in London requesting he carry out secret urgent transactions.

It was only when he joined a 5 minute long online meeting with his bosses which included a lookalike of the CFO who told him to make the payment that he put his earlier concerns out of his mind.

Unfortunately all those in the meeting apart from the victim were AI generated fakes with very realistic deepfake images and voices.

Reported by Hong Kong Police Force
February 2024

5. Regional Scam Experiences

Interpol's assessment on global financial fraud published in March 2024[17] found the most prevalent scams are investment, advance payment, romance & business email compromise. Regional summaries state:

5.1 Asia:

"*Pig butchering fraud schemes initiated in Asia in 2019, & expanded during the COVID-19 pandemic. Subsequently, Asia has emerged as a focal point, with criminal organisations in poorer countries across the region employing business-like structures. Another fraud type that has experienced a surge in recent years in Asia is a type of telecommunication fraud where perpetrators impersonate law enforcement officers or bank officials to trick victims to disclose their credit card or bank account credentials or to hand over huge amounts of money".*

5.2 Africa:

"Business Email Compromise remains one of the most prevalent trends in Africa, however there is increasing use of the pig butchering fraud. Cases of this fraud type have been identified in West & Southern Africa targeting victims in other jurisdictions beyond the continent. Certain West African criminal groups, incl the Black Axe, Airlords & Supreme Eiye, continue to grow transnationally, & are known to have extensive skills in online financial fraud such as romance fraud, investment fraud, advance fee fraud, & cryptocurrency fraud".

5.3 Americas:

"*The most common types of fraud across the Americas are impersonation, romance, tech support, advance payment, and telecom frauds. Human trafficking-fuelled fraud continues to be a growing crime phenomenon. The INTERPOL coordinated operation, Operation Turquesa V[18], revealed that hundreds of victims were trafficked out of the region after being lured via messaging apps and social media platforms and coerced to commit fraud, including investments frauds and pig butchering. There is emerging evidence that Latin-American crime syndicates such as Commando Vermelho, Primeiro Comando da Capital (PCC) and Cartel Jalisco New Generation (CJNG) are also involved in the commission of financial fraud".*

5.4 Europe:

"Online investment frauds, phishing, and other online financial fraud schemes have escalated on carefully selected targets to maximise profits. Mobile phone apps are also being targeted by cybercriminals. The criminal networks involved in these online schemes often display sophisticated and complex modi operandi, which are usually a combination of different fraud types. Pig butchering, predominantly carried out of call centres in Southeast Asia, is also on the rise".

5.5 Source Countries:

Whilst all countries are source countries for scammers a number of countries often stand out as having significant scam source footprints, including: Nigeria, famed for 419 advance fee frauds as well as stolen credit cards, scams around gold sales & online dating, confidence fraud, false paperwork and & inheritance transfers, fake websites, fake contracts, kidnapping & robbery, & employment scams. Other notorious countries include: India, China, Brazil, Pakistan, Indonesia, Venezuela, South Africa, Philippines & Romania.

Countries that are source and target countries for potential fraud attempts such as spam e mails indicate a concentration in a number of countries, for example, when it comes to spam e mails, 24.77% were sent from Russia. A further 14.12% were sent from Germany. The top 5 origin countries for spam emails in 2021 were: Russia (24.77%), Germany (14.12%), USA (10.46%), China (8.73%) & Netherlands (4.75%). Countries receiving the highest spam emails every day were topped by the USA (8 billion), Czech Republic (7.7 billion), Netherlands (7.6 billion). France (7.5 billion), Russia (7.4 billion), Germany (7.1 billion) & Canada (7 billion), Ukraine (7 billion) China (7 billion and the UK (6.9 billion)[19].

Asia

“Pig butchering fraud schemes initiated in Asia in 2019, & expanded during the COVID-19 pandemic. Subsequently, Asia has emerged as a focal point, with criminal organisations in poorer countries across the region employing business-like structures. Another fraud type that has experienced a surge in recent years in Asia is a type of telecommunication fraud where perpetrators impersonate law enforcement officers or bank officials to trick victims to disclose their credit card or bank account credentials or to hand over huge amounts of money”.

Source: Interpol 2024

6. Scam Reports on Australia, Hong Kong SAR and Singapore

The GCFFC APAC Chapter established a Scams working group in 2023 to review the scam threats and responses in the APAC Region, focussing on Australia, Hong Kong SAR and Singapore.

Reports on findings are included in this report in Section 7 - Australia, Section 8 - Hong Kong SAR and Section 9 - Singapore. Reports and data have also been assessed to generate overall key findings in Section 10 below.

A comparative analysis of Scam KPI/KRI data for Australia, Hong Kong SAR and Singapore is set out below.

Comparative Analysis - Proceeds of Crime/Victim Losses - Scams in Australia Hong Kong & Singapore			
	Australia	Hong Kong SAR	Singapore
Proceeds/Losses			
Proceeds/Losses from 2023	AU$2.74 Billion -13% from 2022	HK$9 Billion	S$651.8 M (-1.3% from 2022)
Proceeds/Losses from 2022	AU$3.15 Billion +79% from 2021	HK$4.8 Billion	S$660.7M (+4.5% from 2021)
Proceeds/Losses from 2021	AU$1.8 Billion	N/A	S$632M (+137.9% from 2020)
Proceeds/Losses from 2020	AU$851 Million	HK$3.5 Billion	S$265.7M (+55.6% from 2019)
Proceeds/Losses from 2019	AU$634 Million	HK$2.65 Billion	S$170.8M
US Dollars Proceeds/Losses 2023	US$1.88 Billion	US$1.16 Billion	US$482 Million
Average US$ per victim	US$3,128 (A$4,565)	US$29,000 (HK$226,000)	US$10,514 (S$14,189)
Average US$ per person	US$72 (A$107)	US$155 (HK$1,200)	US$83 (S$112)
As %age of Country GDP	0.1% (US$1.7 Trillion)	0.3% (US$360 Billion 2022)	0.1% (US$$467 Billion 2022)
Main Scams by Losses 2023	INV, RA, BEC, ROM, PHISH	INV, IMPER, JOB, FFRIEND, ECOM	INV, JOB, IMPER, ROM, MAL
Main Scams % Total 2023 Losses	74%	N/A	78%
Trend	Improving	Worsening	Slightly Improving
Cases			
Number of Reported Cases 2023	601,000 (+18.5% from 2022)	39,824 (+42.6% from 2022)	46,563 (+ 46.8% from 2022)
Population experience of Scam	2.5% (2023)	0.53% (2023)	0.79% (2023)
Cases from 2022	507,284 (-% from 2021)	27,923 (+45% from 2021)	31,728 (+ 32.6% from 2021)
Cases from 2021	566,648 (-11% from 2020)	19,259 (+24% from 2020)	23,933 (+ 52.9% from 2020)
Cases from 2020	444,164 (+21.5% from 2019)	15,553 (+89.3% from 2019)	15,651 (+ 64% from 2019)
Cases from 2019	167,000	8,216 (-1.9% from 2018)	9,545
Main Scams by Cases 2023	INV, RA, BEC, ROM, PHISH	INV, IMPER, JOB, FFRIEND, ECOM	JOB, ECOM, FFRIEND, PHIS, INV
Main Scams % Total 2023 Cases	N/A	68%	78%
Total Crime Rate in 2023	N/A	90,276 (70,048)	70,242 (53,662 in 2022)
Scams % of Total Crime in 2023	N/A	44% (40% in 2022)	66% (59% in 2022)
Trend	Worsening	Worsening	Worsening

Australia
Scam Assessment

Australians suffered losses in 2023 of AU$2.7 Billion (US$1.66 Billion) from 601,000 reported cases, down from AU$3.15 Billion from 507,284 reported cases in 2022

Source:Australian Competition and Consumer Commission (ACCC)

7. Australia

According to the Australian Competition and Consumer Commission (ACCC), in its Targeting Scams Report for 2023[20], published in April 2024, it estimated that Australians suffered losses in 2023 of **AU$2.7 Billion (US$1.88 billion)** from **601,000** reports, down from **AU$3.15 Billion** from **507,284** cases in 2022. The recent trend on losses is "**improving**" with the first decline after significant increases over the last 5 years, though cases continue to trend as "**worsening**". For overall Australia Scam KPI/KRI's, see below:

7.1 Australia Scam KPI/KRI's

Australia Scam KPI/KRI's highlights from 2019 - 2023:

Scam KPI/KRI's			
Description	**Proceeds/Losses**	**Description**	**Cases**
Proceeds/Losses from 2023	**AU$2.74 Billion -13% from 2022**	**Number of Reported Cases 2023**	**601,000 (+18.5% from 2022)**
Proceeds/Losses from 2022	**AU$3.15 Billion +79% from 2021**	**Cases from 2022**	**507,284 (- from 2021)**
Proceeds/Losses from 2021	**AU$1.8 Billion**	**Cases from 2021**	**566,648 (-11% from 2020)**
Proceeds/Losses from 2020	**AU$851 Million**	**Cases from 2020**	**444,164 (+21.5% from 2019)**
Proceeds/Losses from 2019	**AU$634 Million**	**Cases from 2019**	**167,000**
US Dollars Proceeds/Losses 2023	**US$1.88 Billion**	**Population experience of Scam**	**2.5% (2023)**
Average US$ per victim	**US$3,128 (A$4,565)**	**Main Scams % Total 2023 Cases**	**N/A**
Average US$ per person	**US$72 (A$107)**	**Total Crime Rate in 2023**	**N/A**
As %age of Country GDP	**0.1% (US$1.7 Trillion)**	**Scams % of Total Crime in 2023**	**N/A**
Main Scams by Losses 2023	**INV, RA, BEC, ROM, PHISH**	**Main Scams by Cases 2023**	**INV, RA, BEC, ROM, PHISH**
Main Scams % Total 2023 Losses	**74%**		
Trend	**Improving**	**Trend**	**Worsening**
Sources: Australian Government sources including Targeting Scams Annual Reports by ACCC			

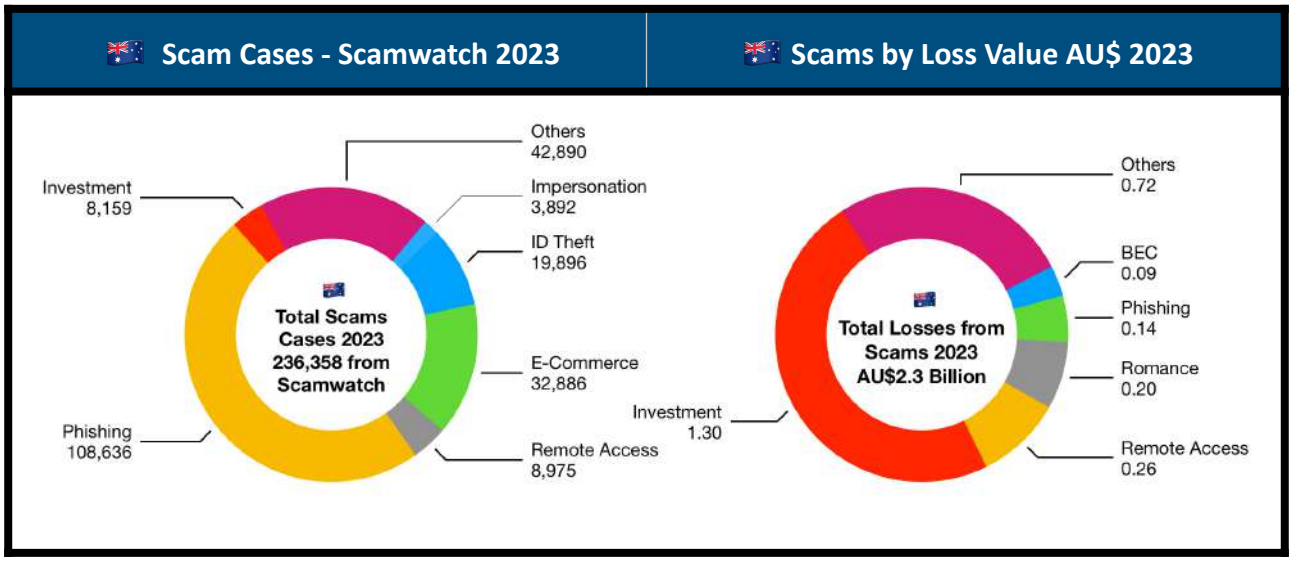
Australia Scam KPI/KRI's highlights include:

- An estimated **AU$2.7 billion** (US$1.88 billion) in losses in **2023** represents
    - a first reduction in losses in 2023 by **13%** are the first since recent reports began
    - approx **0.1%** of Australian GDP
    - an average loss per victim of **AU$4,565** (US$3,128) & **A$107** per capita (US$72)
- An estimated **601,000** cases in 2023 represents
    - another increase up **18.5%** from 2022 and up from **167,000** in 2019
    - the most common financial related crime in Australia
    - approx **2.5%** of Australians reported experiencing scams

7.2 Australian Scams in more detail

Additional Australia Scam KPI/KRI's highlights include:

- Investment scams caused the most financial loss, with combined losses of AU$1.3 billion followed by:
    - remote access scams with AU$229 million lost
    - romance scams with AU$200 million
    - phishing scams at AU$140 million &
    - Business E Mail Compromise scams (the most common scam type for small business) at AU$90 million
- Phishing scam cases were reported at 108,636 in 2023 (according to Scamwatch) followed by:
    - e commerce scams with 32,886 cases
    - ID theft scams with 19,896 cases
    - remote access scams with 8,975 cases
    - investment scams with 8,159 cases



7.3 Australia Scam Inherent Risk Assessment

Age and other attributes do make a difference when it comes to scams, in terms of prevalence and success, for example according to reports from including with reference to Australia's Scamwatch data in 2023:

- **Wealthy Population:** Australia is a wealthy country, with an average US$64,491 GDP per capita (PPP) compared to the global average of US$12,647 GDP per capita (PPP). This makes Australia a target rich environment for bad actors, who can enjoy relatively higher profit per victim as compared with many other nations. This is especially the case for the older generations of Australians, who are more likely to have realised gains in the property market and substantial superannuation balances which are less encumbered after reaching preservation age.
- **Older Australians:** Those 65+ years age continue to lose more money than other age groups. Scammers take advantage of some older people's lack of technology knowledge and experience, as well as other

vulnerabilities including loneliness. The ACCC has highlighted that scammers are specially targeted dating sites and social media for older Australians who have recently divorced or lost a long-term partner, taking advantage of those who are inexperienced with these sites and may be in a vulnerable emotional state. Those 65+ years of age also looking to grow their money have been found to be vulnerable to investment scams where the scammers have invested time and money into convincing sales pitches, flashy websites, & even glossy brochures. Older Australians are also disproportionately affected by remote-access scams.

- **Generation Z:** Younger generations (born 1997 - 2012), driven by curiosity & a propensity for risk-taking, often believe that they are able to detect and avoid scams and that scams will not affect them personally, which renders them vulnerable. The time spent online by this generation (social media, shopping, games) is making them more susceptible to scams. They are more inclined than people in older age brackets to engage with virtual assets (buy/sell as well as ICOs), leaving them susceptible to investment scams. Additionally, scammers are using social media platforms and email as forums for sextortion scams, where they threaten to share intimate images or footage online, unless demands are met. Scammers are also targeting children who play online video games by offering unlocked achievements or special items in exchange for money or gift card codes without ever transferring the item.

- **Culturally and linguistically diverse (CALD) communities:** Australia has a significant proportion of cultural and linguistic diverse communities who are vulnerable to impersonation scams (from impersonated public officials) and online scams. These consumers may not be easily accessible by standard government engagement channels which makes it more difficult to provide necessary awareness and advice. Nevertheless use of the English language is the dominant and common language which is the overwhelming language for the internet, and likely most targeted as a result by other English speaking fraudsters.

- **Indigenous Australians:** Due to lower internet literacy rates indigenous Australians may be more vulnerable to scams. They are often a by scammers offering to assist in obtaining disaster relief or other government payments for them for an upfront fee.

- **Digital Factors:** A number of digital factors will influence also the risks and vulnerabilities for Australians, for example:

  - As at January 2024 the population of the world is approximately at 8.08 billion, of which 5.61 billion or 69.4% of the total population have mobile phones, 5.35 billion or 66.2% of the total population use the internet & 5.04 billion or 62.3% of the total population use social media. With 2 billion aged between 0-14, the percentages of 15 year olds and above would increase the above percentages to 93.5%, 89% & 84% respectively. The respective figures for or Australia are 124%, 96% & 81% for 2023[21].

  - And for 16-64 yr olds, 6H 40M is spent on average globally on the internet, with older age groups spending more time than younger age groups with the equivalent figures for Australians being 5H 51M

  - And for 16-64 yr olds, 2H 3M is spent on average on social media, with younger age groups spending more time than older age groups, with the equivalent figures for Australians being 2H 04M.

  - Cash usage for payments is at 16% globally compared to Australia at 13%

  - Online banking usage at 27.7% globally (use per month) compared with Australia at 40,1%

  - Nearly half of all scam losses were processed through cryptocurrency exchanges, which is not so surprising when you consider crypto-confidence is high (Australia has the third-highest rate of crypto adoption in the world according to CoinDesk at 17.9%)[22].

  - Confirmation of Beneficiary is not yet mandatory in Australia for any payment channel.

  - Faster instant payments were introduced in Australia in 2018 for domestic payments. The 'NPP' (New Payments Platform) allows for account to account "real time" payments. 'Osko,' which is run by

Australia's national bill payment system BPAY, checks all attempted account to account payments to determine whether or not both the sending and receiving account are enabled for NPP real time payments. If both accounts are enabled for NPP, then the payment will be sent via NPP instead of BECS, meaning it is essentially instantaneous.

- **Digital Enablers and Businesses:** Based on reporting to Scamwatch[23] the most prevalent contact method for scammers targeting victims in 2023 were by:

  - Text Message (109,621 reports and AU$26.9 in related losses)
  - Phone Calls (55,418 - related losses AU$116 M)
  - Email (85,941 - related losses AU$80 M)
  - Social Media (17,542 - related losses AU$80.2 M)
  - Internet (17,568 - related losses AU$73.5 M)
  - Mobile Apps (8,101 - related losses AU$64.8 M)
  - In person (3,614 - related losses AU$21.5 M)

Major increases in contact usage can be seen for email, social media, on the internet and by text message in 2023. Many job and investment scams rely on adverts and posts on social media as well as direct engagement using apps such as WhatsApp. With many disruption activities focused on phone and SMS text messaging this only highlights the need for professional digital enablers and businesses to take proactive steps to disrupt scammer misuse of their services. These findings have also led to the Australian government consult on a proposal for Mandatory Industry Scam Codes. For more see below.

- **Data Security:** Australian citizens have endured a spate of large scale high profile data breaches from 2022 onwards, which have exposed the personal information and identity credentials of millions of Australians including many leaked identity documents, thereby making them more prone to identity theft and social engineering attacks, which in turn leads to making opening fake accounts, account takeover and mule accounts to launder scam proceeds far easier for bad actors and for redirect transactional accounts or even interfering in payments from tax or superannuation.

- **Cyber Crime:** According to the Organised Crime Index 2023[24],"*Cybercrime in Australia is a growing threat and has evolved significantly as the use of digital and communications technologies by Australians increases. Cybercriminals are becoming more sophisticated and are targeting a wider range of victims, including businesses, hospitals and government agencies. Ransomware is a significant threat, causing serious harm to victims and the broader community. Australia has increased its efforts to prevent and investigate cybercrime but faces challenges due to the dynamic nature of the risk and the difficulty of investigating transnational crimes. Ransomware attacks are increasingly common and often difficult to deter or reduce*" AND that, *"Financial crimes, specifically in the form of cyber-enabled financial crime, is a growing problem in Australia, with millions of Australian dollars being funnelled to cybercriminals every year through fraudulent online schemes. The proliferation of smartphones, social media, new payment technologies and online platforms has made it easier for cybercriminals to refine their strategies and engage with potential victims. Most financial frauds involve limited contact with a victim, making it difficult for individuals to identify such illicit activities and take proactive steps to protect themselves*".

- **Fraud & Money Laundering Risk:** Fraud has been identified as one of the main predicate offences to Money Laundering of most concern in Australia, alongside other serious crimes such as drugs and arms trafficking, corruption, people smuggling, theft and tax offences. An increasing driver of scams in Australia is the availability of accounts through which to quickly siphon funds, made possible through both fraudulently obtained documents as well as a large cohort of willing or deceived "**money mules**". There appears to be an abundance of mules, some of whom are themselves co-opted via romance scams and job scams and transformed into unwitting accomplices quickly moving and withdrawing illicitly gained funds. Australia's foreign student and migrant populations are also vulnerable and often used as money mules (wittingly or unwittingly).

7.4 Australia Scam Inherent Risk Assessment Dashboard - In more detail

Australia represents higher inherent scam risks based on an assessment of factors as set out below:

Scams Risk Assessment - Inherent Risk			
Risk Area	**Lower Risk**	**Moderate Risk**	**Higher Risk**
1. Inherent Risks - Inherent Vulnerabilities - Economic			
1.1 GDP Per Capita Average (Av US$12,647 - 2022)	N/A	N/A	US$64,491 2022 estimate
2. Inherent Risks - Inherent Vulnerabilities - Digital/Online/Social Media			
1.2 Global Mobile Phone Usage (Av usage at 69.4% / 93.5% - Adult)	N/A	N/A	124.3% - Mobile Connections
1.3 Global Internet Usage (Av usage at 66.2% / 89% - Adult -2023)	N/A	N/A	96.2% Adult usage
1.4 Global Social Media Usage (Av usage at 59.4% / 84% - Adult - 2023)	N/A	81% Adult usage	N/A
1.5 Time spent online (globally Av - 6H 37M - 2023)	5H 51M	N/A	N/A
1.6 Time on social media (globally at 2H 3M - 2023)	N/A	N/A	2H 4M
3. Inherent Risks - Inherent Vulnerabilities - Finance including Payments			
1.7 Cash for Payments (16% global av - 2022)	N/A	N/A	13% usage of Cash for payments
1.8 Online Banking use (2023) (Banking App Monthly use - 27.7%)	N/A	N/A	40.1%
1.9 Confirmation of Beneficiary (Mandatory for Main Bank/FI's)	N/A	In progress and to be rolled out nationally	N/A
1.10 Fast/Inst Payments (F/IP) (F/IP available/Can Banks/FIs legally slow higher risk payments)	N/A	F/IP available domestically since 2018 / Banks vary re inserting friction	N/A
4. Inherent Risks - Inherent Vulnerabilities - Scam Ecosystem Identified			
1.11 Scam Ecosystem Digital Enablers/Businesses	N/A	N/A	Scam ecosystem banks, telco's, digital platforms, and cryptocurrency exchanges, social media and dating sites - ACCC NASC 2024
5. Other Inherent Risk / Vulnerability Factors			
1.12 Data Security / Breaches (Cybersecurity standards/Major Breaches)	N/A	N/A	Major Security Data Breaches since 2022
1.13 Language (Main Languages Spoken & Understood)	N/A	N/A	English Speaking more attractive target for fraudsters
1.14 NRA - Fraud ML Risk	N/A	N/A	Fraud one of higher risk predicate crimes from NRA 2011
1.15 Cyber Dependent Crime (OC Index 2023)	N/A	N/A	Australia is rated 7.5/10

7.5 Australia Scam Response

Australia has the vision to be the "*hardest target for scammers",* in the world[25]. Australia's lead agency targeting scams, the Australian Competition and Consumer Commission (ACCC) has stated that, "*more coordinated effort is required across government, the private sector & law enforcement to combat scams. Businesses need to be vigilant & implement effective monitoring & intervention processes to prevent scammers using their services & stop them when they do. Identity, verification & communication processes need constant review as scammers constantly evolve. We need to arm consumers with the tools to give them the best chance to identify scams, whilst recognising that humans aren't going to stop being human any time soon. Put simply, we need solutions that stop scammers reaching consumers & makes it harder for them to get access to money from the bank accounts of ordinary Australians"*[26]. Major initiatives and actions include:

- **Reporting:** Comprehensive annual reporting in the form of "Targeting Scams Reports", published by the ACCC, with the latest covering 2023[27], published in April 2024, with the first annual report published in 2010, reporting on 2009. Scam reports are received into the NASC mostly into Scamwatch and by ASIC and the AFCX (see below).

- **The Fintel Alliance:** The Fintel Alliance was established in March 2017[28], and is led by AUSTRAC as a public–private partnership with the objective to help grow Australia's economy and protect it from criminal exploitation. The Fintel Alliance brings together experts from financial institutions, state and commonwealth law enforcement and intelligence agencies, as well as academic and research institutions. The purpose of the Fintel Alliance is to: Protect the financial system from criminal abuse and exploitation by enhancing information sharing & innovative capability development through a trusted, collaborative partnership between government and industry.

- **Anti Scam Centre:** A new **National Anti-Scam Centre** (NASC) was established in July 2023[29], within the ACCC, with new government funding of AU$57M over 3 years, focusing on an ecosystem approach to scam prevention and detection. It brings together government law enforcement and the private sector to disrupt and prevent scams through data and intelligence gathering and enhancing public awareness and education. The NASC has performance targets which is reported on to report on benefits gained from its establishment and functioning. The NASC also houses Scamwatch[30] which shares information from scam reports received by the NASC, including issuing warnings and other reports and awareness raising activities. It is also a reporting centre

- **Scam Awareness:** The Annual Scams Awareness Week was first run in 2018. It is an initiative of the scams awareness network (a group of government regulatory agencies and departments in Australia and New Zealand responsible for consumer protection and policing in the areas of scams, cyber safety and fraud). The 2023 Scams Awareness Week was held in November 2023[31], delivered via the ACCC with the theme 'Who's really there?'. The campaign was successfully delivered in collaboration with members of a Scams Awareness Network through media releases, paid media advertising, and organic social media content reaching millions of Australians.

- **Banks & Other FI's:** Australian Banks & FI's are on a journey to design & implement increasingly effective anti scam programmes, leveraging new technology as well as wide-ranging expertise. Benchmarking current Anti Scam Programmes (ASP) to best practices provides Banks and FI's with opportunities to close any gaps where risks are high & controls are not yet effectively mitigating these risks. For more on what best practice ASP for Banks/FI's may look like, contact the GCFFC secretariat, which has collated a best practice guide. Key actions & initiatives relating to Australian Banks & FI's include as follows:

  - **Regulatory Supervision:** ASIC, the financial regulator has also increased its Independent reviews of Banks and other FI's scam prevention, detection and response including on-site inspections. It summarised findings from its report[32], "*Scam prevention, detection and responses by the four major banks in April 2023. It reported that between 1 July 2021 and 30 June 2022, more than 31,700 customers of the 4 major banks collectively lost more than* ***A$558 million*** *through scams. This was an increase of 49% in customers and 50% in financial losses compared to the previous 12-month period.*

During the same period, Banks paid approximately A$21 million in reimbursement and/or compensation payments to customers who fell victim to a scam, representing just 3.7% (range of 2-5%) of the total amount in terms of value and 11% in terms of cases. The big 4 Banks prevented A$109M or 13% (range of 5 -18%) of total estimated Bank related fraud and scams". The ACIP also found varying responses to counter fraud with just one Bank at that time having a comprehensive anti fraud strategy, with others work in progress and overall mostly rating individual elements as being partially implemented. The review covered areas such as strategy, governance and reporting, preventing, detecting and stopping scams, responding to scam and scam victims & liability, reimbursement and compensation. Areas that were strongest in terms of implementation were Board oversight and awareness programmes for customers, with the remaining focus areas deemed not yet implemented or partially implemented.

- **Scam-Safe Accord:** In November 2023 Australia's community owned banks, building societies, credit unions and commercial banks agreed the "Scam-Safe Accord"[33], which represents a comprehensive set of anti scam measures, to be implemented across the entire banking industry. There are 6 key initiatives which include, i) the delivery of an industry wide confirmation of payee solution to customers for domestic payments, ii) action to tackle ID fraud, including by the end of 2024 introducing at least 1 biometric check for new customers, iii) the introduction of questions, prompts &/or warnings to customers, for example when sending money to new payees or when raising payment limits & imposing delays in executing payments if needed, iv) the expansion of the AFCX and the Fraud Reporting Exchange (within AFCX) to all Banks in Australia to help Banks rapidly share information about scams to prevent scams and to recover funds scammed, v) higher risk channels will be targeted and restrictions introduced by Banks, for example certain cryptocurrency exchanges and or higher risk countries, and vi) establishing an anti scam strategy to improve oversight of the detection and response to scams.

- **Mandatory Codes:** See below as the Banks have also been included in the Australian governments consultation paper on Mandatory Industry Scam Codes[34].

- **The Australian Financial Crimes Exchange (AFCX):** The AFCX[35] was established in 2016 by the largest 4 Australian Banks which helps them to collaborate and coordinate their intelligence and data sharing activities for the investigation and prevention of financial and cyber crime. Scams are reported by ,to AFCX and intelligence provided back to the Banks, and reporting is made to the NASC. The AFCX provides a Fraud Reporting Exchange which is a shared portal for fraud prevention and reporting.

- **Professional Digital Enablers:** The Australian government released a consultation paper on Mandatory Industry Scam Codes[36] on 30 November 2023. The proposal outlines the roles and responsibilities for government, regulators and the private sector in addressing the growing prevalence of scams in Australia. This includes ensuring that key sectors in the scams ecosystem have measures in place to prevent, detect, disrupt, and respond to scams, including via sharing scam intelligence across and between sectors. The initial sectors proposed to be covered by the framework are banks (see above), Telco's (see below) & digital communications platforms, with scope for further sectors to be designated in the future.

- **Telco's:** Australia's telecommunications sector is involved in tacking fraud and scams, and is subject to regulation and supervision by ACMA. Australian Telco's blocked 246 million scam calls & over 106 million scam SMS during Oct - Dec 2023. In order to deal with **SMS alpha tag spoofing** further efforts are needed, including from the telecommunications companies and aggregators, to ensure Alpha Tags used in the SMS cannot be used by anyone else. An SMS Sender ID registry is currently in a pilot phase.

- **International Co operation:** Australian regulators have worked well with international counterparts on a bilateral basis for many years (see for example the scams awareness network with New Zealand authorities mentioned previously). On 12 March, 2024[37], the Australian government attended a first of a kind Global Anti Fraud Summit in London, U.K., attended by G7 countries, as well as South Korea & New Zealand which issued a communique promising further international co operation and collaboration.

7.6 Overall KPI's on Prevention & Recovery Etc: Australia has not published targets and doesn't have specific KPIs on prevention or recovery rates etc.

7.7 Liability & Reimbursement

In Australia, there is no rule or regulation which requires Banks or other 3rd parties to reimburse victims losses from scams. Generally, Australian banks maintain a policy of not automatically refunding victims of fraud, which leaves many victims shouldering the loss. In ASIC's Report[38] of 4 Big Banks it found that reimbursement rates averaged just 3.7%. Whilst some would like to see bank reimbursement requirements put into law, others, like Financial Services Minister Stephen Jones take a different view when in 2022[39] he cited the risk of creating *"a honeypot for scammers"* as a reason for opposing bank liability.

7.8 Australia Scam Response Risk Assessment Dashboard - In more detail

Australia's response has recognised that scams are a serious issue & and a response is underway. Progress is being made, with more still to be done. For more details see the response assessment Dashboard below:

Response including Cross Sector Contributions - Government, LEA, Finance & Digital Enablers - Australia			
Response	**Higher Level of Response**	**Moderate Level of Response**	**Lower Level of Response**
1. Government			
1.1 Anti Fraud Strategy	Australia is prioritising tacking fraud and scams including A$57 for National Anti Scam Centre (NASC) opened in 2023	N/A	N/A
1.2 Lead Anti Fraud Agency	Aus Competition & Consumer Commission (ACCC) ASIC for FI's/ACMA for Telco's)	N/A	N/A
1.3 Government Targets	Australia has vision to be the "*hardest target for scammers*" - NASC has Targets	N/A	N/A
1.4 Reporting	ACCPR Reports using its Annual "Targeting Scams Report" 2021, 2022, 2023 & Qtr's	N/A	N/A
1.5 Awareness Campaign's	Scam Awareness Week in 2020, 2021 and 2022 & "Who's really there" in Nov 2023	N/A	N/A
1.6 PPP Collaboration (E.g. Anti Scam Centre/ Private to Private)	National Anti Scam Centre opened 2023 / Australian Financial Crimes Exchange (AFCX) is a private sector members org	N/A	N/A
2. Police & Law Enforcement			
1.7 Policing Priority to tackle Scams	N/A	N/A	The Australian Federal Police have a more limited role in tackling scams in Australia
1.8 Clean up rates (>2% of reported cases)	Data not available	Data not available	Data not available
1.9 Victim Loss Recovery - LEA (est by GASA on average globally - 7%)	N/A	Check GASA Australia	N/A
3. Finance including Banks and FI's / Telco's			
1.10 FI Anti Fraud Programme (Clarity on AFP obligations/status)	N/A	Mostly "Partially Implemented" Key findings Scam Prevention & Detection Review of Banks (Big 4) published 2023 May 2022/ Feb 2023 by ASIC	N/A
1.11 FI Prevention Rates	N/A	N/A	13% - range of 5% to 18% Banks (Big 4) prevented A$109M of US$845M - scam attempts (yr to June 2022)
1.12 Reimbursement Rates	N/A	N/A	3.7% - range of 2% to 5% & in 11% of cases Bank (Big 4) customers lost A$558M & paid out A$23M (yr to June 2022)
1.13 Awareness Campaigns	Top 4 Banks had Fraud and scam awareness programmes aimed at their customers	N/A	N/A
1.14 Telco's	Blocked 246 million scam calls & over 106 million scam SMS during Oct - Dec 2023 / SMS Sender ID registry in pilot phase	N/A	N/A
4. Digital Enablers and Businesses			
1.15 Codes of Conduct/ Robust Anti Fraud Programmes	N/A	N/A	No Codes in place - Proposed Mandatory Codes expected after Consultation

7.9 Key Findings & Recommendations

This assessment of Australia, with assessments of Hong Kong & Singapore have generated insights which have been translated into possible findings & actions that will be consulted on. See Section 10 below.

Hong Kong Scam Assessment

Hong Kong citizens suffered losses of HK$9 Billion (US$1.16 Billion) from 39,824 reports in 2023, up from HK$4.8 Billion from 27,923 cases in 2022

Source: Hong Kong Police Force (HKPF)

8. Hong Kong SAR

According to the Hong Kong Police[40] it estimated that Hong Kong citizens suffered losses in 2023 of **HK$9 Billion** from **39,824** reports, up from **HK$4.8 Billion** from **27,923** cases in 2022. The recent trend on reported losses is significantly "**worsening**" with record highs with cases also "**worsening**". For overall Hong Kong Scam KPI/KRI's, see below:

8.1 Hong Kong Scam KPI/KRI's

Hong Kong Scam KPI/KRI's highlights from 2019 - 2023:

🇭🇰 Scam KPI/KRI's			
Description	**Proceeds/Losses**	**Description**	**Cases**
Proceeds/Losses from 2023	**HK$9 Billion (+95% from 2022)**	**Number of Reported Cases 2023**	**39,824 (+42.6% from 2022)**
Proceeds/Losses from 2022	**HK$4.8 Billion**	**Cases from 2022**	**27,923 (+45% from 2021)**
Proceeds/Losses from 2021	**N/A**	**Cases from 2021**	**19,259 (+24% from 2020)**
Proceeds/Losses from 2020	**HK$3.5 Billion**	**Cases from 2020**	**15,553 (+89.3% from 2019)**
Proceeds/Losses from 2019	**HK$2.65 Billion**	**Cases from 2019**	**8,216 (-1.9% from 2018)**
US Dollars Proceeds/Losses 2023	**US$1.16 Billion**	**Population experience of Scam**	**0.53% (2023)**
Average US$ per victim	**US$29,000 (HK$226,000)**	**Main Scams % Total 2023 Cases**	**68%**
Average US$ per person	**US$155 (HK$1,200)**	**Total Crime Rate in 2023**	**90,276 (70,048)**
As %age of Country GDP	**0.3% (US$360 Billion 2022)**	**Scams % of Total Crime in 2023**	**44% (40% in 2022)**
Main Scams by Losses 2023	**INV, IMPER, JOB, FFRIEND, ECOM**	**Main Scams by Cases 2023**	**INV, IMPER, JOB, FFRIEND, ECOM**
Main Scams % Total 2023 Losses	**N/A**		
Trend	**Worsening**	**Trend**	**Worsening**
Sources: Hong Kong Government & Police sources			

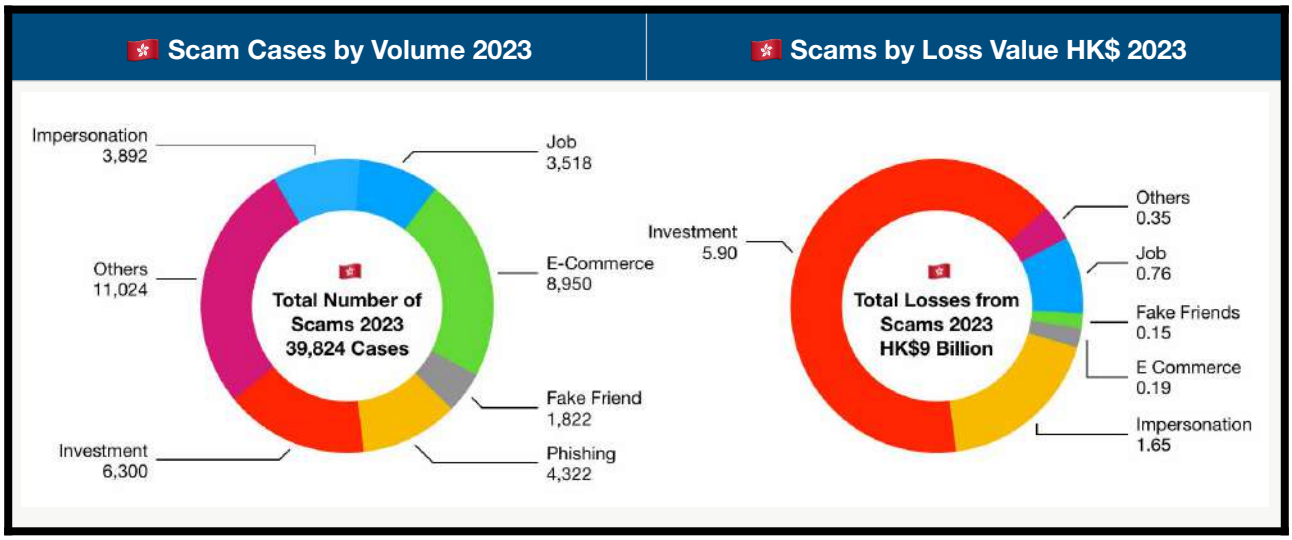
Hong Kong Scam KPI/KRI's highlights include:

- An estimated **HK$9 billion** (US$1.16 billion) in losses in **2023** represents
    - a significant increase in losses in 2023 by **95%** and at record levels
    - approx **0.3%** of HK GDP
    - an average loss per victim of **HK$226,000** (US$29,000) & **HK$1,200** per capita (US$155)
- An estimated **38,824** cases in 2023 represents
    - another increase up **42.6%** from 2022 and up from **8,216** in 2019
    - the most common financial related crime in Hong Kong
    - approx **0.5%** of Hong Kong citizens are victims of scams

8.2 Hong Kong Scams in more detail

Additional Hong Kong Scam KPI/KRI's highlights include:

- Investment scams caused the most financial loss in 2023, with combined losses of HK$5.9 billion followed by:
    - impersonation scams with HK$1.65 billion lost
    - job scams with Hk$760 million lost
    - e commerce scams with HK$190 million
    - fake friends with Hk$150 million
- e commerce scams with 8,950 cases were reported the most often in 2023 followed by:
    - investment scams with 6,300 cases
    - phishing scam cases were reported at 4,322
    - e commerce scams with 8,950 cases
    - job scams with 3,518 cases, &
    - fake friend with 1,822 cases



8.3 Hong Kong - Scam Inherent Risk Assessment

Age and other attributes do make a difference when it comes to scams, in terms of prevalence and success, for example:

- **International Financial Centre**: Hong Kong is one of the worlds largest international and regional financial centres attracting capital and investment from mainland China and overseas, due not least to low crime and corruption rates, the safety and soundness of its banking sector and strong financial infrastructure. Whilst these factors attract capital and wealth, they also attract criminal syndicates from overseas. These

syndicates aim to exploit the city's customers and financial system for illicit activities and thereafter quickly transfer funds scammed abroad.

- **Wealthy Population:** Hong Kong is wealthy, with an average US$69,072 GDP per capita (PPP) compared to the global average of US$12,647 GDP per capita (PPP). This makes Hong Kong a target rich environment for bad actors, who can enjoy relatively higher profits per victim as compared with many other nations.

- **Age Distribution of Victims:** E-shopping scams target individuals who are less familiar with online shopping or have limited experience with e-commerce platforms. In the first half of 2023, e-shopping fraud affected individuals ranging in age from 11 to 76 years old. Job scams primarily target job seekers, including individuals who are desperate for employment or seeking remote work opportunities. According to the HKPF, young people who are eager to secure job opportunities may be particularly susceptible due to their limited experience and eagerness to enter the job market. Phishing scams often target individuals who are less tech-savvy or unaware of common phishing tactics. In Q1 2023, a significant proportion of phishing scam victims (nearly 25% of the total) were between the ages of 51 and 60. Investment scams often target individuals who are seeking financial gains or looking for lucrative investment opportunities. In the first three quarters of 2023, victims of online investment scams varied in age from 13 to 80 years old, indicating that individuals of any age, gender, educational level, and background can fall victim to these scams. However, it is notable that the largest age group of victims comprises middle-aged individuals between 46 and 55 years old, accounting for 25% of the total victims. These individuals have a certain level of financial capability and knowledge. Many of them are professionals, including doctors, professors, surveyors, accountants, and investment advisors. Telephone deception often targets vulnerable populations, particularly the elderly or individuals who may be more trusting or easily intimidated. In 2022, approximately 80% of the victims targeted by telephone deception were aged 60 and above.

- **State institutions and Capabilities**: An effective anti scam response has to come from government and ministries, which includes embracing governments role as one that is predicated as “by the people for the people”, and the same are empowered and enabled to bring forward anti scam measures and solutions and ensure they are enforced and implemented properly. Hong Kong rates well in taking such actions and is likely to be an asset rather than a vulnerability.

- **Digital Factors:**

A number of digital factors will influence also the risks and vulnerabilities for citizens of Hong Kong, for example:

- As at January 2024 the population of the world is approximately at 8.08 billion, of which 5.61 billion or 69.4% of the total population have mobile phones, 5.35 billion or 66.2% of the total population use the internet & 5.04 billion or 62.3% of the total population use social media. .With 2 billion aged between 0-14, the percentages of 15 year olds and above would increase the above percentages to 93.5%, 89% & 84% respectively. The respective figures for Hong Kong are 223.7%, 93.1% & 89.9% for 2023.

- And for 16-64 yr olds, 6H 26M is spent on average globally on the internet, with older age groups spending more time than younger age groups with the equivalent figures for Hong Kongers being 6H 26M

- And for 16-64 yr olds, 2H 3M is spent on average on social media, with younger age groups spending more time than older age groups, with the equivalent figures for Hong Kongers being 1H 52M.

- Cash usage for payments is at 16% globally compared to Hong Kong at 11%

- Online banking usage at 27.7% globally (use per month) compared with Hong Kong at 42%

- **Digital Enablers and Businesses:** Based on reporting by the Hong Kong Police[41], in the first half of 2023, scammers in Hong Kong pretended to be sellers and posted fake advertisements on:

- Facebook (60%)
- Carousell (23%)
- WhatsApp (5%) &
- Instagram (4%)

With many disruption activities focussed to date more on phone and SMS Text Messaging this only highlights the need for professional digital enablers and businesses to take proactive steps to disrupt scammer misuse of their services.

- **Data Security:** Hong Kong's privacy watchdog, the Office of the Privacy Commissioner for Personal Data (PCPD) reported that more than 150 data breach notifications were made in 2023[42] marking a nearly 50% increase compared to the previous year. A total of 157 cases of hacking, loss of documents, inadvertent disclosure of personal data, and other types of data breach were also reported. The figure increased by almost 50% compared to 105 notifications received in 2022. Privacy Commissioner for Personal Data Ada Chung said that the rise could be attributed to two large-scale data leak incidents, which raised awareness of the threat. "*[The incidents] prompted organisations and corporations to be more cautious. When information was leaked, they would report to us at the earliest opportunity*," Chung said. In September, 2022, Cyberport reported[43] that sensitive data such as staff details and credit card records had been disclosed following a "malicious" hack in Mid August. In the same month, the Consumer Council fell victim to hackers who launched a cyberattack that damaged about 80% of the watchdogs computer systems[44].

- **Fraud ML Risk:** Fraud was identified in the National AML Risk Assessment in 2018[45] as one of the main predicate offences to Money Laundering of most concern in Hong Kong, alongside other serious crimes such as Drugs offences and externally (international), Corruption & Tax offences. The most recent NRA published in 2022[46] identified the overall threat from ML as "medium high", with fraud as the most prevalent financial crime affecting Hong Kong, with other serious offences, drugs, corruption, tax crimes, serious gambling offences, goods smuggling and the illegal wildlife trade also highlighted, along with goods piracy and loansharking, people smuggling, blackmail, theft and burglary. The NRA 2022 stated that, "*fraud-related crime encompasses a variety of criminal activities. Fraud-related crime accounts for almost 16% of total number of reported crime cases in Hong Kong from 2016 to 2020, the largest share of reported crime portfolio during the period. Study of cases between 2016 and 2020 revealed the following types of major fraud related-predicate crime – (a) Online business fraud, e.g. e-shopping fraud and online commercial fraud; (b) Email scam (both business and personal), e.g. hacking and pretence; (c) Social media deception, e.g. romance scam, compensated dating scam; (d) Online miscellaneous fraud, e.g. bogus investment plan, online employment scam; and (e) Telephone deception, e.g. "Pretend Government Officials", "Guess Who" and "Detained Son" scam. Analysis of ML investigations commenced between 2016 and 2020 revealed that fraud-related crimes took up the majority (about 70%) of the identified predicate crimes. The ratio of domestic fraud-related offences to external fraud-related offences account is about 40:60. The amount of proceeds involved in external foreign fraud-related crime is of much larger size. Among the convicted ML cases, fraud-related crime takes up a substantial percentage in the number of cases and proceeds involved from 2016 to 2020. For example, 80.6% of property restrained and 18.8% of property confiscated between 2016 and 2020 were proceeds connected to fraud-related offences. The ratio of convicted ML cases with domestic and foreign fraud cases was similar. Still, the amount involved in the domestic fraud-related predicate was more substantial than the foreign fraud-related predicate".*

- **Money Mules/Stooges:** The use of individual and corporate stooge accounts are prevalent in fraud-related crimes, with the deposit of large sums which is often quickly followed by withdrawals to overseas third parties which have no apparent relation with the depositor, a main typology. For domestic fraud-related crimes, the principal offenders would either deal with the proceeds through mules/stooges, associates or even family members. In external fraud cases, mule/stooge accounts are used by cross-border syndicates to move money quickly across the globe. The entry of new institutions such as SVF licensees and VB's in recent years, and technological advances such as the Faster Payment System ("FPS"), while facilitating faster and more convenient services for legitimate customers, have been targeted by

scammers. From detected ML cases, individual accounts are often opened by the criminals themselves, family members or associates, and by mules/stooges, who may or may not be Hong Kong residents. Corporate accounts of legitimate businesses may be exploited, or accounts set up by shell companies to hide beneficial ownership. Among all the ML cases involving bank accounts, most of the accounts were used for a temporary repository of funds, i.e., the funds transferred into the account would be transferred away within a short period, and usually to somewhere outside of Hong Kong. This method suggests that Hong Kong was often involved mainly in the early stage of the ML process, i.e. "placement and layering". Hong Kong actively promotes financial technology and financial inclusion, making it relatively easy to open bank accounts physically or remotely in the city. However, this accessibility is exploited by criminals who recruit money mules to open bank accounts and receive fraudulent funds. As a result, the use of such mule accounts remains a common method for laundering fraud-related funds within the banking sector. There appears to be an abundance of mules, some of whom are themselves co-opted via romance scams and job scams and transformed into unwitting accomplices quickly moving and withdrawing illicitly gained funds. Hong Kong's foreign student and migrant populations are also vulnerable and often used as money mules (wittingly or unwittingly).

- **New Digital Products, Services and Channels**: In recent years, the finance sector in Hong Kong has introduced new products and services such as virtual banks and stored value facilities, remote account opening, and faster instant payments. While these services provide convenience to customers, criminals exploit the easy access to digital banking and instant payment services, available 24/7, to carry out scams and transfer out scammed funds. Electronic payment channels, including online banking and mobile banking platforms like the FPS, provide convenience for money transfers. However, these channels can also be exploited by fraudsters to move illicit funds. Remote customer onboarding allows individuals to open bank accounts without physically visiting a bank branch. While this process offers convenience for customers, it can also be exploited by criminals for money laundering activities. Criminals may recruit stooges, individuals who impersonate legitimate customers, to open bank accounts or obtain financial services illicitly.

- **Virtual Currency:** Hong Kong citizens are well aware of virtual currencies (91%), with approx 31% having holdings of VC themselves[47]. Whilst fraudsters and scammers utilise VC to transfer their illicit criminal proceeds, they also target VC holdings for scam attempts. In addition, the Asia Pacific region and especially the region's global financial centres, including Hong Kong face increasing concerns about cryptocurrency and blockchain money laundering fuelled by North Korean cybercrime.

In a recent case which made headlines, a Hong Kong employee of a UK company has become the poster child for the harm that can come from the use by scammers of deep fake technology. For more details see the box below.

A recent “business e mail compromise” type scam with a big modern twist was reported by the Hong Kong Police in January 2024. A finance department employee based in HK of a UK headquartered engineering company, Arup, HK$200 Million (US$25 Million) to a 3rd party - a scammer. He had already received a suspicious email purportedly from the Company’s HQ in London requesting he carry out a secret urgent transaction. It was only when he joined a 5 minute long online meeting with his bosses which included a lookalike of the CFO who told him to make the payment that he put his concerns out of his mind. Unfortunately all those in the meeting apart from the victim were AI generated and very realistic deepfake images and voices.

8.4 Hong Kong Scam Inherent Risk Assessment Dashboard - In more detail

Hong Kong represents higher inherent scam risks based on an assessment of factors as set out below:

Scams Risk Assessment - Hong Kong 🇭🇰			
Inherent Risk/Inherent Vulnerabilities			
Risk Area	**Lower Risk**	**Moderate Risk**	**Higher Risk**
1. Inherent Risks - Inherent Vulnerabilities - Economic			
1.1 GDP Per Capita Av PPP (Av US$12,647 - 2022)	**N/A**	**N/A**	**US$69,072 GDP 2023**
2. Inherent Risks - Inherent Vulnerabilities - Digital/Online/Social Media			
1.2 Global Mobile Phone Usage (Av usage at 69.4% / 93.5% - Adult)	**N/A**	**N/A**	**223.7% - Mobile Connections**
1.3 Global Internet Usage (Av usage at 66.2% / 89% - Adult -2023)	**N/A**	**N/A**	**93.1% Adult usage**
1.4 Global Social Media Usage (Av usage at 59.4% / 84% - Adult - 2023)	**N/A**	**N/A**	**89.9% Adult usage**
1.5 Time spent online (globally Av - 6H 37M - 2023)	**N/A**	**N/A**	**6H 26M**
1.6 Time on social media (globally at 2H 3M - 2023)	**1H 52M**	**N/A**	**N/A**
3. Inherent Risks - Inherent Vulnerabilities - Finance including Payments			
1.7 Cash usage for Payments (16% global av - 2022)	**11% usage of Cash for payments**	**N/A**	**N/A**
1.8 Online Banking use (2023) (Banking App Monthly use - 27.7%)	**N/A**	**N/A**	**42%**
1.9 Confirmation of Beneficiary (Mandatory for Main Bank/FI's)	**N/A**	**N/A**	**Not Mandatory**
1.10 Fast/Inst Payments (F/IP) (F/IP available/Can Banks/FIs legally slow higher risk payments)	**N/A**	**N/A**	**F/IP since 2014 for domestic and some international - India Malaysia etc**
4. Inherent Risks - Inherent Vulnerabilities - Scam Ecosystem Identified			
1.11 Scam Ecosystem Digital Enablers/Businesses	N/A	N/A	**Scam ecosystem** Banks, telco's, technology, digital platforms, e commerce & cryptocurrency exchanges, social media dating & adult sites
5. Other Inherent Risk / Vulnerability Factors			
1.12 Data Security / Breaches (Cybersecurity standards/Major Breaches)	**N/A**	**N/A**	**Major Security Data Breaches in 2022**
1.13 Language (Main Languages Spoken & Understood)	**N/A**	**N/A**	**Cantonese & English**
1.14 NRA - Fraud ML Risk	**N/A**	**N/A**	**Fraud higher - NRA 2018**
1.15 Cyber Dependent Crime (OC Index 2023)	**Hong Kong is not included**	**Hong Kong is not included**	**Hong Kong is not included**

8.5 Hong Kong Scam Response

Tackling scans in Hong Kong is not a new priority. For example, the 24/7 stop-payment mechanism operated under Anti-Deception Coordination Centre (ADCC) of the Hong Kong Police was launched in 2017, as was the public-private information sharing platform Fraud and Money Laundering Intelligence Taskforce (FMLIT), the HKMA AML Regtech Lab was launched in 2021, the anti-fraud search engine "Scameter" operated by the HKPF launched in September 2022, the Financial Intelligence Evaluation Sharing Tool (FINEST) established in June 2023, & the Anti-Scam Consumer Protection Charter launched was launched in June 2023. Even more recently the establishment of the Anti-Deception Alliance announced in November 2023 and The Office of the Communications Authority (OFCA) SMS Registration Scheme was announced in December 2023.

The Hong Kong government has stated:

- in 2018[48] that "*The Government will spare no efforts and devote the necessary resources to ensure that Hong Kong stays as safe and clean place for living work and doing business*", and

- in 2022[49] that that "*The Government is committed to ensuring that HK remains one of the worlds safest and cleanest cities to work do business and enjoy life*".

- in 2024[50] the HKMA have confirmed tackling fraud remains one of its main strategic priorities for 2024 and has proposed and is consulting on providing additional Bank to Bank information sharing gateways beyond corporate account details to include individual account details too with safeguards.

Major initiatives and actions include:

- **Reporting:** Regular reporting by the Hong Kong Police[51] on crimes generally affecting Hong Kong, which includes substantial coverage of so called "deception" or scam related cases have been published, including covering 2023 and earlier years, so that data covering 2019 - 2023 is publicly available.

- **Anti Scam Centre:** To combat actions against scams and increase public awareness, the Hong Kong Police Force set up the Anti-Deception Coordination Centre (ADCC) under the Commercial Crime Bureau with a view to consolidating all the relevant efforts of the Force in fighting and preventing the crime. The ADCC was established in July 2017[52] and operates an all day enquiry hotline "Anti-Scam Helpline 18222", which provides immediate advice for the general public and enhanced support to frontline units of the HKPF in order to handle scam cases in a more effective manner. Citizens can refer to the ADCC website for the latest scam trends and typologies. The ADCC also takes responsibility for strategy in relation to scams, for enhancing co ordination amongst agencies and internationally and co ordinates anti-scam publicity and education campaigns. It also monitors and analyses the trend of deception cases, provides risk evaluation, and takes timely actions in response. Since the ADCC's formation in 2017, 864 deception cases identified by Bank staff have been successfully intervened, 700 fraudsters arrested and illicit funds worth more than Hk$12.3 billion (US$1.57 billion) intercepted as a result of close collaboration with the banking industry. In order to take collaboration to the next level, the **Anti Deception Alliance (ADA)** was formed in November 2023[53]. It signifies the shared vision of the Hong Kong Police Force (HKPF), Hong Kong Monetary Authority (HKMA) and banking industry to "*combat deception, safeguard the financial interests of Hong Kong citizens and uphold the reputation of Hong Kong as an international financial hub*". The new ADA will see representatives from 10 major banks assigned to work with officers from the ADCC to provide "*real-time assistance*" in tackling fraudulent activities and boosting "*strategic intelligence exchange*" between the HKPF and the banks to "*more effectively identify emerging fraudulent activities & their associated risks in order to facilitate the formulation and implementation of corresponding counter-measures to mitigate such risks*". A further aim is to "*provide an interactive platform for the participating banks to facilitate the sharing of best practices in anti-deception strategies to establish a safer & more reliable financial environment".* Since the establishment of the ADA, the average response time of banks in intercepting fraudulent payments significantly reduced by 70%. HKMA chief executive Eddie Yue described the alliance's launch as " another important milestone for public private partnerships in combating "fraud and financial crime", saying that, *rapid and effective communication and intelligence-sharing will assist the banking industry to detect and prevent fraud risk and related mule account networks, as well as helping intercept fraudulent payments more effectively*."

- **Scam Awareness:** In recent years, HKPF have organised a series of publicity campaigns and used multiple channels to raise public awareness of scam trends. These include placing advertisements on mass media, public transport and outdoor billboards; and launching the online portal "**Cyber Defender**"[54]. Besides, the HKPF have also collaborated with the HKMA and the banking industry to launch various promotional campaigns via the Internet, social media platforms and bank branches to raise public awareness on fraudulent activities. Another awareness raising tool, is "**Scameter"**[55] which is an anti-fraud search engine operated by the HKPF launched in September 2022, It allows the public to search various data (including bank account numbers, SVF user IDs and phone numbers) and provides a coloured risk-rated response. Where the inputted data is linked to scams, Scameter helps alert the public to the potential level of risk before making payments or conducting transactions which could potentially expose them to prevalent types of fraud, such as online shopping fraud, investment fraud and romance scams. As of December 2023, the search engine has recorded over 2.13 million searches and issued nearly 360 000 alerts on frauds and cyber security risks.

- **Banks and Other FI's:** Hong Kong Banks and FI's are on a journey to design and implement effective and sustainable anti scam programmes, recognising few countries Banks' and FI's have yet achieved close to maturity, effectiveness or sustainability in this area and doing so will take quite some time. Nevertheless benchmarking current Anti Scam Programmes to best practices provides Banks and FI's with opportunities to identify and close any gaps particularly where inherent risks are high and controls are not yet effectively mitigating these risks. For more details on what best practice anti fraud programmes for Banks/ Fi's may look like, contact the GCFFC secretariat, which has collated a best practice guide. Key actions and initiatives relating to Hong Kong Banks & FI's are also included under regulatory supervision below.

  - **Regulatory Supervision:** HKMA, the financial regulator has also increased its focus on scams and how the financial services sector they regulate can respond.

    - In April 2023[56] the HKMA with the HKPF and 28 retail banks in April 2023, it was agreed that anti-scam efforts in Hong Kong needed enhancing. 5 areas were targeted in the areas of real-time fraud monitoring, bank-to-bank information sharing, suspicious proxy identifier (ID) alert model, and the enhancement of 24/7 stop payment controls.

    - On 13 October 2023[57] the HKMA sent a letter to Bank CEOs informing them of additional expectations including that FIMLIT (see below) & FINEST (see below) membership would be expanded, expectations about real time scam monitoring, customer alerts on faster payments.

    - The HKMA also published a circular on 31 October 2023[58] requiring all Authorised Institutions (AIs) announced to implement e-banking enhancements no later than 31 March 2024. These measures including i) Enhanced monitoring for suspicious transactions and additional customer authentication to combat fraud, ii) Empowering customers to safeguard bank accounts, & iii) Containing damage to customers in case of serious breaches.

    - AMLab is a recurring event, comprising a series of AML Regtech Labs which was launched by the HKMA in November 2021 as an interactive and collaborative platform for banks, industry experts, and technology companies to share knowledge, experience, and new ideas on AML Regtech adoption and implementation. The HKMA's fourth AMLab event held on 7 June 2023[59] sought to explore innovative fraud monitoring and detection solutions aligned to the HKMA and HKPF joint initiative. In this session, the HKMA shared with the participants the joint initiative requirements for real-time fraud monitoring and how the discussions can support further technology adoption within their banks. All retail banks and major Stored Value Facility (SVF) licensees, alongside Regtech vendors and international experts, shared their perspectives on the future of Hong Kong's anti-fraud regime – focusing on the critical role that technology will play in helping banks on the front line of defence.

      Following AMLab 4, a 'Regtech Connect' networking session was held, where vendors offering fraud detection and analytics solutions met with local banks to explore further collaboration opportunities. A key theme explored at AMLab 4 was the balance between anti-fraud processes and providing customers with a seamless banking experience.

- In June 2023[60] the HKAB and the HKMA jointly launched the Anti-Scam Consumer Protection Charter (the Charter), all 23 card issuing banks and 15 merchant institutions in Hong Kong participated in the Charter. Under the Charter, Participating Institutions commit not to send instant electronic messages (e.g. SMS, WhatsApp, WeChat, etc.) to customers with embedded hyperlinks to request for personal and credit card information online, and to convey the message of "Beware of scams" to the public through various channels. Finally, banks will provide contact information through official channels to allow customers to verify message senders identities as well as message authenticity. Fourth, banks will provide frontline staff with enhanced training to handle customer enquiries. The HKAB agreed to will closely monitor the latest trends and methods used in credit card scams while conducting public education campaigns to boost customer confidence in credit card payments. With all the measures introduced, customers can enjoy the convenience of spending with credit cards." The HKAB also established a special task force in the first quarter of this year to drive the implementation of protective measures for credit card holders. These include banks setting up dedicated teams for the handling of fraud cases, and continuously enhancing the capability of staff to deal with such cases. The banking industry will also upgrade online services and mobile apps to provide stronger protection for customers, such as allowing customers to set credit limits for card-not-present (CNP) transactions and to suspend their credit cards instantly with a single click.

- The HKMA issued a public consultation paper on 23 January, 2024[61] seeking views on its proposal to allow Authorised Institutions (AIs) to share information on customer accounts for the purposes of preventing and detecting financial crime, in particular in response to the sharp global increase in digital fraud. In addition to the harm caused to victims, large-scale digital fraud could undermine public confidence in the use of new digital financial services. Information sharing is internationally recognised as an effective tool in addressing financial crime. The HKMA notes that the United States, United Kingdom and Singapore have information sharing gateways. While Hong Kong has achieved positive outcomes through public-private information sharing partnerships, criminals' exploitation of the financial system to move illicit funds continues to pose a threat. There is a need for faster sharing of information to further support the advanced use of technology and analytics to detect and disrupt fraud and mule account networks and intercept illicit funds more effectively. In Hong Kong, participating AIs can share information on corporate accounts with one another through the Financial Intelligence Evaluation Sharing tool ("FINEST") launched in June 2023. However FINEST currently does not support information sharing on personal accounts due to concerns over data privacy. The Consultation Paper points out that FINEST's ability to prevent and detect crime would be enhanced if information sharing were extended to personal accounts because a significant portion of mule account networks involve bank accounts held by individuals.

- The HKMA published its strategic priorities for 2024[62] which included focusing on anti fraud measures in addition to AML and financial crime risk. According to the HKMA, safeguarding customers is paramount for FIs, ensuring trust, compliance, and sustainable business operations amid evolving regulatory requirements. On anti fraud, the focus will be on, **pre-emotive & agile responses to digital fraud**: Ensuring e-banking security keeps up with fraud landscape; monitoring banks' implementation of new e-banking security measures; stepping up surveillance, **Collaboration:** Further enhance effectiveness of 5 joint anti-fraud initiatives (see above); expansion of Anti-Scam Consumer Protection Charter; **Strengthening Defences:** Against digital frauds with banks and police, **Education and Promotion**: Latest modus operandi, Mobile point-of-sale terminals, public education **Innovation:** Adoption of network analytics to strengthen real-time fraud monitoring; enhancing suspicious proxy alert model. Banks are expected to continue to evaluate and develop current anti fraud operations: Learn how to keep your organisation safe with effective anti-fraud measures.

- **PPP's:** Fraud & ML Intelligence Taskforce (FIMLIT): In 2017[63], HKPF, HKMA and the banking sector jointly established the FIMLIT for exchanging intelligence and updating banks with the most recent fraud typologies. Currently, members of FMLIT include the HKPF, the Independent Commission Against Corruption, the Customs and Excise Department, and 28 retail banks in Hong Kong, including all eight virtual banks. Since its inception, 10 Banks (Including HSBC, Bank of China, SCB, Hang Seng Bank & ICBC) came together and through information sharing and data analytics, banks identified over 31,500 previously unknown mule accounts since establishment, and took prompt actions while supporting law

enforcement investigations. This collaboration helped increase the number of intelligence-led suspicious transaction reports by 319% in 2022 compared with 2021, leading to an increase of 113% in criminal proceeds restrained or confiscated. Assets frozen/ restrained / confiscated related to FMLIT intelligence amounted to HKD 1267.1 M as of Dec 2023. In line with international experience, banks in Hong Kong continued to be the major contributor accounting for over 84,781 suspicious transaction reports (or over 85% of the total) filed in 2023, which provided timely and actionable intelligence assisting criminal investigations.

- **Financial Intelligence Evaluation Sharing Tool (FINEST):** In June 2023[64], the pilot phase of the Financial Intelligence Evaluation Sharing Tool (FINEST) was launched. The initiative was developed by the Hong Kong Association of Banks (HKAB) with guidance from the HKMA and support from the HKPF for a cyber-secured platform to speed up the bank-to-bank sharing. The pilot phase of FINEST covering five domestic systemically important Authorised Institutions (D-SIBs) sharing information on corporates suspected to be involved in fraud-related money laundering activities. Based on the experience of the pilot phase and making reference to international experience, FINEST will be expanded to cover more banks and a wider scope of financial crimes and accounts. The HKMA is expected to consult the industry and the public on legal provisions to facilitate personal account information sharing for preventing and detecting crime.

- **Professional Digital Enablers:** Whilst a number of countries have passed laws requiring certain digital businesses, such as technology, search, mail, social media, e commerce etc to take action to keep people safe online and or are introducing industry codes, Hong Kong has yet to propose specific actions. This despite evidence from the HKPF[65], in the first half of 2023, that of those scammers targeting Hong Kong and who pretended to be sellers and posted fake advertisements, these could be founds mostly on Facebook (60%), followed by Carousell (23%), WhatsApp (5%) and Instagram (4%). To intercept scams at their source, the HKPF requested Facebook to remove over 5,200 accounts related to fraud in the first half of 2023. Approximately 90% of these accounts were successfully removed.

- **Telco's:** Hong Kong's telecommunications sector is involved in tacking fraud and scams, and is subject to regulation and supervision by **The Office of the Communications Authority (OFCA).** In order to prevent spoofing of Bank SMS messages to customers, a scheme has been implemented since 28 December 2023[66], so that members of the public receiving SMS in Hong Kong can easily identify whether the SMS is from a Registered Sender, for example a Bank. The main sectors that have registered their sender ID's are the Banking sector, the Telecommunications sector & the Government bureau / departments, statutory bodies or other related organisations[67].

- **International Co operation:** On 12 March, 2024[68], first of a kind Global Anti Fraud Summit was held in London, U.K., attended by G7 countries, as well as South Korea & New Zealand which issued a communique promising further international co operation and collaboration. Hong Kong was not in attendance.

8.6 Overall KPI's on Prevention & Recovery Etc

Hong Kong has not published targets and doesn't have specific KPIs on prevention or recovery rates etc.

8.7 Liability & Reimbursement

In Hong Kong, under the Code of Banking Practice, unless a customer acts fraudulently or with gross negligence, he should not be responsible for any direct loss suffered by him as a result of unauthorised transactions conducted through his account. However, the interpretation of "gross negligence" can be subject to debate and may vary in different situations.

8.8 Hong Kong Scam Response Risk Assessment Dashboard - In more detail

Hong Kong's response has recognised that scams are a serious issue and that whilst the response is underway and whilst progress has been made, more is still to be done and initiatives and actions need to

Singapore Scam Assessment

Singapore's citizens suffered losses of SGD 651.8 Million (USD 482 Million) from 46,563 cases in 2023, slightly down from S$660.7 Million from 31,728 cases in 2022.

Source: Singapore Police Force (SPF)

deliver to address the threat. For more details on Hong Kong's response see the response risk assessment Dashboard below:

Response including Cross Sector Contributions - Government, LEA, Finance & Digital Enablers - Hong Kong			
Response	**Higher Level of Response**	**Moderate Level of Response**	**Lower Level of Response**
1. Government			
1.1 Anti Fraud Strategy	Hong Kong is prioritising tacking scams including expanding PPPs & tackling identified scam related weaknesses	N/A	N/A
1.2 Lead Anti Scam Agencies	HK Police Force - Commercial Crime Bureau & HKMA	N/A	N/A
1.3 Government Targets	N/A	N/A	No Specific Targets Set
1.4 Reporting	Regular reporting from HKPF on cases and losses and by types	N/A	N/A
1.5 Awareness Campaign's	Scam prevention and Anti Phishing Campaigns in 2023 & Scameter (since 2023	N/A	N/A
1.6 PPP Collaboration (E.g. Anti Scam / Private to Private)	Anti Deception Coordination Centre (since 2017), & FINEST ADAlliance & FMLIT Expansion (since 2017)	N/A	N/A
2. Police & Law Enforcement			
1.7 Policing Priority to tackle Scams	Anti Deception Coordination Centre (Since 2017) supported by ADAlliance (since 2023)	Data not available	Data not available
1.8 Clean up rates	Data not available	Data not available	Data not available
1.9 Victim Loss Recovery - LEA (est by GASA on average globally - 7%)	Data not available	Recovery est by GASA at 7.8% for full, 1.1% for a substantial & 3.3% partial (2022)	Data not available
3. Finance including Banks and FI's / Telco's			
1.10 FI Anti Fraud Programme (Clarity on AFP obligations/status)	Banks & FI's AFP Responsibilities / Expectations increasingly detailed by HKMA	N/A	N/A
1.11 FI Prevention Rates	HK$12.3 billion (about £1.25bn/US$1.57bn) "intercepted" connected to ADCC	N/A	N/A
1.12 Reimbursement Rates	N/A	Banking Code - reimbursement unless customer is fraudulent or grossly negligent	N/A
1.13 Awareness Campaigns	All major Banks regularly educate and make customers aware of Scams	N/A	N/A
1.14 Telco's	N/A	Supporting SMS Registration Scheme & Other SMS related initiatives	N/A
4. Digital Enablers and Businesses			
1.15 Codes of Conduct/ Robust Anti Fraud Programmes	N/A	N/A	No Codes No Mandatory Responsibilities

8.9 Key Findings & Recommendations

This assessment of Hong Kong, together with assessments of Australia and Singapore have generated insights which have been translated into possible findings and actions that will be consulted on as set out in Section 10 below.

9. Singapore

According to the Singapore Police Force[69], it is estimated that Singapore's citizens incurred losses of S$651.8 Million (approximately US$482 Million) in 2023, slightly down from S$660.7 Million in 2022. Cases in 2023

were reported at 46,563, representing a 46.8% increase from the previous year. The recent trend in financial losses shows a marginal improvement with 2023 witnessing the first decline after significant increases over the last 5 years. However, the number of cases continues to escalate, indicating a worsening situation. For overall Singapore Scam KPI/KRI's, see below:

9.1 Singapore Scam KPI/KRI's

Singapore Scam KPI/KRI's highlights from 2019 - 2023:

Scam KPI/KRI's			
Description	**Proceeds/Losses**	**Description**	**Cases**
Proceeds/Losses from 2023	S$651.8 M (-1.3% from 2022)	Number of Reported Cases 2023	46,563 (+ 46.8% from 2022)
Proceeds/Losses from 2022	S$660.7M (+4.5% from 2021)	Cases from 2022	31,728 (+ 32.6% from 2021)
Proceeds/Losses from 2021	S$632M (+137.9% from 2020)	Cases from 2021	23,933 (+ 52.9% from 2020)
Proceeds/Losses from 2020	S$265.7M (+55.6% from 2019)	Cases from 2020	15,651 (+ 64% from 2019)
Proceeds/Losses from 2019	S$170.8M	Cases from 2019	9,545
US Dollars Proceeds/Losses 2023	US$482 Million	Population experience of Scam	0.79% (2023)
Average US$ per victim	US$10,514 (S$14,189)	Main Scams % Total 2023 Cases	78%
Average US$ per person	US$83 (S$112)	Total Crime Rate in 2023	70,242 (53,662 in 2022)
As %age of Country GDP	0.1% (US$$467 Billion 2022)	Scams % of Total Crime in 2023	66% (59% in 2022)
Main Scams by Losses 2023	INV, JOB, IMPER, ROM, MAL	Main Scams by Cases 2023	JOB, ECOM, FFRIEND, PHIS, INV
Main Scams % Total 2023 Losses	78%		
Trend	Slightly Improving	Trend	Worsening
Sources: Singapore Government sources including Singapore Police Force			

Singapore An estimated **S$651 million** (US$482 million) in losses in **2023** representing:

- A first reduction in losses in 2023 by **1.3%** and the first since recent reports began
- Approximately **0.1%** of Singapore GDP
- An average loss per victim of **S$14,189** (US$10,514) & **S$112** per capita (US$83)

- An estimated **46,563** cases in 2023 representing:
  - An increase of **46.8%** from 2022 and up from **9,545** in 2019
  - The most common financial related crime in Singapore
  - Approximately 0.79**%** of Singaporeans who report being victims of scams

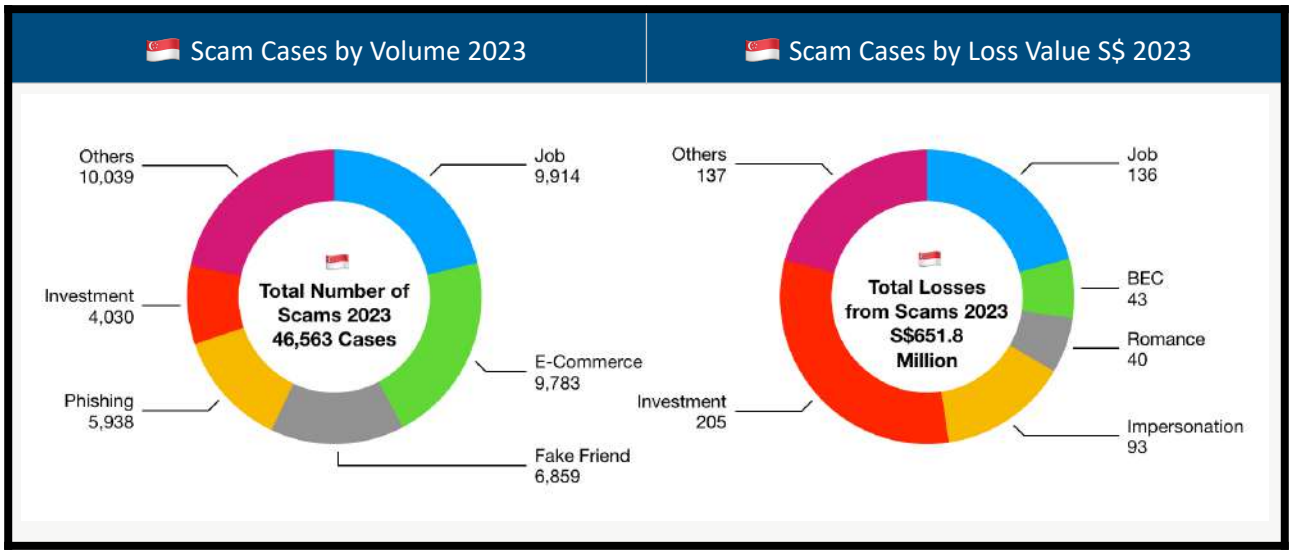
9.2 Singapore Scams in more detail

Additional Additional Singapore Scam KPI/KRI's highlights include:

- Investment scams resulted in the highest financial loss, totalling S$204.5 million
- Job scams followed with losses amounting to S$135.7 million
- Government officials impersonation scams had significant losses of about S$92.5 million
- Business Email compromise scams at S$43 million
- Romance scams with S$40 million lost

In terms of case numbers for 2023:

- Job scam cases were the most prevalent at 9,914
- E-commerce scams were a close second with 9,783 cases
- Fake friend scams were reported 6,859 times
- Phishing scams occurred in 5,938 cases
- Investment scams were reported at 4,030 cases



9.3 Singapore Scam Inherent Risk Assessment

Singapore's status as a wealthy nation with an advanced economy and high digital connectivity contributes to its vulnerability to scams. Despite being one of the world's safest countries with low crime rates and robust financial governance, Singapore faces challenges from international fraud and scams. Relevant considerations for risks and vulnerabilities include:

- **Wealthy Population:** Singapore's GDP per capita (PPP) was S$113,779 (approximately USD 84,500) in 2023, significantly higher than the global average, making it an attractive target for fraudsters seeking higher profits per victim.

- **Demographics:** Scammers often target both young adults and the elderly. In 2023, individuals aged below 50 accounted for 73% of scam victims. Youths (aged 19 and below) comprised 5.3% of scam victims, with a notable percentage falling prey to e-commerce and job scams. Adults (aged 30 to 49) represented 43.1% of scam victims, with e-commerce and job scams being prevalent. Seniors (aged 50 and above) were less affected but remained vulnerable to specific scams such as fake friend call scams.

- **Cost of Living:** Economic pressures, including a potential economic downturn and rising living costs, have heightened financial insecurity, which scammers exploit, particularly through job, investment, and e-commerce scams.

- **Cultural and Linguistic Diversity:** Singapore's multicultural and multilingual society, with official languages including English, Malay, Mandarin, and Tamil, presents opportunities for scammers to target various communities.

- **Digital Factors:** A number of digital factors will influence also the risks and vulnerabilities for Singaporeans, for example:

  - As at January 2024 the population of the world is approximately at 8.08 billion, of which 5.61 billion or 69.4% of the total population have mobile phones, 5.35 billion or 66.2% of the total population use the internet & 5.04 billion or 62.3% of the total population use social media. .With 2 billion aged between 0-14, the percentages of 15 year olds and above would increase the above percentages to 93.5%, 89% & 84% respectively. The respective figures for Singapore are **162%, 96%** & **85%** for 2023[70].

  - And for 16-64 yr olds, **6H 26M** is spent on average globally on the internet, with older age groups spending more time than younger age groups with the equivalent figures for Singaporeans being **6H 49M**

  - And for 16-64 yr olds, 2H 3M is spent on average on social media, with younger age groups spending more time than older age groups, with the equivalent figures for Singaporean's being **2H 14M**

  - Cash usage for payments is at 16% globally compared to Singapore at **19%**

  - Online banking usage stands at **34.2%** monthly, with **34.9%** of Singaporeans using a payment app.

- **New Digital Products, Services, and Channels:** The financial sector in Singapore regularly introduces innovative services such as virtual banks, stored value facilities, and remote account opening, which offer convenience but also present new opportunities for criminal exploitation. Instant payment services like FAST (Fast And Secure Transfers established in 2014 and near real-time cross-border payment options with a number of countries including India, Malaysia and Thailand,) are particularly vulnerable to misuse by fraudsters for scamming and money laundering activities. The ease of remote customer onboarding, while beneficial, can be manipulated by criminals to create fraudulent accounts or access financial services.

- **Digital Enablers and Businesses:** Digital Enablers and Businesses that provide services such as mail, telephone, SMS, online and social media messaging, and e-commerce are often leveraged by scammers. The Singapore Police Force Annual Scams Report for 2023[71], indicates that out of a total of 9,783 e-commerce scam cases, the top five digital platforms used were:

  - Facebook with 4,550 cases (46.5%),
  - Carousell with 2,476 cases (25.3%),
  - Telegram with 787 cases (8%),
  - [Platform X] with 299 cases (3.1%), and
  - WhatsApp with 243 cases (2.5%).

  This highlights the need for professional digital enablers and businesses to take proactive steps to disrupt scammer misuse of their services.

- **Data Security:** Despite strong cyber and data security standards, Singapore has not been immune to large-scale data breaches. High-profile incidents, such as the SingHealth cyberattack in 2018, which

compromised the personal data of 1.5 million patients, highlight the ongoing challenges in protecting sensitive information.

- **Fraud/Scam ML Risk:** Fraud and scams are recognised as significant predicate offences leading to money laundering in Singapore. While the National Risk Assessment of 2014 highlighted concerns such as Criminal Breach of Trust (CBT) and foreign corruption, the current landscape shows a marked increase in scams involving "money mules." These individuals, often co-opted through romance or job scams, unwittingly assist in moving and withdrawing illicit funds. Singapore's diverse foreign student and migrant populations are particularly susceptible to being exploited as mules. The Organised Crime Index 2023[72] reports a surge in cyber-dependent crimes, including ransomware attacks, with small and medium-sized enterprises being common targets. Despite these challenges, Singapore's law enforcement agencies have demonstrated effectiveness in combating financial crimes, conducting operations that have led to the arrest of numerous scammers and the dismantling of scam syndicates.

  Virtual Currency: Awareness of virtual currencies is high among Singaporeans, with a notable portion holding virtual currency assets and 13.6% engaging with virtual currencies[73]. While these digital assets can be used legitimately, they are also targeted by scammers and pose a risk for money laundering, especially in the context of the Asia Pacific's financial centres. The region faces challenges from sophisticated cybercrime, including activities linked to North Korean entities.

9.4 Singapore Scam Inherent Risk Assessment Dashboard - In more detail

Singapore represents higher inherent scam risks based on an assessment of factors as set out below:

Scams Risk Assessment - Singapore 🇸🇬			
Risk Area	**Lower Risk**	**Moderate Risk**	**Higher Risk**
1. Inherent Risks - Inherent Vulnerabilities - Economic			
1.1 GDP Per Capita Average (Av US$12,647 - 2022)	**N/A**	**N/A**	**US$109,000 2023 estimate**
2. Inherent Risks - Inherent Vulnerabilities - Digital/Online/Social Media			
1.2 Global Mobile Phone Usage (Av usage at 69.4% / 93.5% - Adult)	**N/A**	**N/A**	**162% - Mobile Connections**
1.3 Global Internet Usage (Av usage at 66.2% / 89% - Adult -2023)	**N/A**	**N/A**	**96% Adult usage**
1.4 Global Social Media Usage (Av usage at 59.4% / 84% - Adult - 2023)	**N/A**	**85% Adult usage**	**N/A**
1.5 Time spent online (globally Av - 6H 37M - 2023)	**N/A**	**N/A**	**6H 49M**
1.6 Time on social media (globally at 2H 3M - 2023)	**N/A**	**N/A**	**2H 14M**
3. Inherent Risks - Inherent Vulnerabilities - Finance including Payments			
1.7 Cash for Payments (16% global av - 2022)	**19% usage of Cash for payments**	**N/A**	**N/A**
1.8 Online Banking use (2023) (Banking App Monthly use - 27.7%)	**N/A**	**N/A**	**34.2%**
1.9 Confirmation of Beneficiary (Mandatory for Main Bank/FI's)	**TBC**	**TBC**	**Not Mandatory**
1.10 Fast/Inst Payments (F/IP) (F/IP available/Can Banks/FIs legally slow higher risk payments)	**N/A**	**N/A**	**F/IP since 2014 for domestic and some international - India Malaysia etc**
4. Inherent Risks - Inherent Vulnerabilities - Scam Ecosystem Identified			
1.11 Scam Ecosystem Digital Enablers/Businesses	N/A	N/A	**Scam ecosystem** Banks, telco's, technology, digital platforms, e commerce & cryptocurrency exchanges, social media dating & adult sites
5. Other Inherent Risk / Vulnerability Factors			
1.12 Data Security / Breaches (Cybersecurity standards/Major Breaches)	**N/A**	**N/A**	**Major Security Data Breaches in 2018, 2020 & 2021**
1.13 Language (Main Languages Spoken & Understood)	**N/A**	**N/A**	**English Mandarin Malay & Tamil**
1.14 NRA - Fraud ML Risk	**N/A**	**N/A**	**Fraud one of higher risk predicate crimes from NRA 2014**
1.15 Cyber Dependent Crime (OC Index 2023)	**N/A**	**N/A**	**Singapore is rated 6.5/10**

9.5 Singapore Scam Response

Singapore has a well-defined strategy to combat scams outlined by the Ministry of Home Affairs (MHA) in September 2023. This strategy employs a three-pronged approach:

- **Upstream Measures:** These measures aim to prevent scams before they occur. Examples include:
    - ScamShield Mobile App: This app developed by the Singapore Police Force (SPF) filters and blocks scam messages and calls.
    - SMS Sender ID Registry regime: This registry helps identify suspicious senders. Non-registered senders are labelled with a “Likely-SCAM” warning.
- **Downstream Measures:** These measures focus on minimising damage after a scam occurs. This include banking measures implemented in collaboration with Financial Institutions (FI’s).
- **Public Education Initiatives:** The government actively educates the public through advisories and campaigns promoting best practices to identify and combat scams.

9.5.1 Emphasis on Vigilance

Singaporean leaders emphasise the importance of individual vigilance against scams. Mr. Tan Puay Ker, Vice-Chairman of the National Crime Prevention Council (NCPC), highlights the need for precautionary measures. He recommends actions like:

- Downloading the ScamShield App
- Using the Money Lock feature offered by banks to secure savings
- Exercising caution when responding to requests for personal information
- Reporting suspected scams promptly to the Police

These collective actions can significantly reduce the impact of scams within the community.

9.5.2 Shifting Strategy and Ongoing Efforts

Singapore's approach to combatting scams has evolved over time. Initially, the focus was on reactive and targeted measures. In recent years, the strategy has become more proactive and broader in scope. While these efforts have shown effectiveness, the fight against scams is continuous.

David Chew, the Director of the Commercial Affairs Department (CAD) of the SPF, acknowledges the ongoing challenge: "Scams continue to be a key concern". The SPF collaborates with various stakeholders to address this issue, including other government agencies, industry partners, and international law enforcement.

9.5.3 Key Achievements and Future Focus

The Anti-Scam Command (ASCOM), a dedicated unit within the SPF, partners with over 100 stakeholders to fight scams. In 2023, ASCOM's efforts yielded significant results:

- Seizure of close to 20,000 bank accounts
- Recovery of over $100 million in scam funds
- Dismantling of 19 overseas scam syndicates targeting Singapore

The government is also taking legislative steps to address online harms and money mules. Additionally, partnerships with banks have led to the introduction of anti-malware security features in banking apps. Looking ahead, the fight against scams requires a multi-pronged approach. While law enforcement plays a crucial role, a discerning and vigilant public is equally important. The SPF's commitment to collaboration with stakeholders and other government agencies ensures Singapore remains well-equipped to combat this evolving threat.

Major initiatives and actions include:

- **Regular Scam Reporting by the Singapore Police Force (SPF):** The SPF publishes an informative "Annual Scams and Cybercrime Brief" every year as a half yearly report. Both reports provide valuable insights into the latest scam trends and helps the public stay informed. The most recent edition, covering 2023 scams, was published in February 2024[74].

- **The Singapore AML/CFT Industry Partnership (ACIP):** Established in April 2017, ACIP[75] is a public-private partnership committed to combating financial crime in Singapore. It brings together various stakeholders, including, FI's (banks and other relevant firms), Regulators (Monetary Authority of Singapore - MAS), Law enforcement agencies (Commercial Affairs Department - CAD) and other government entities. The structure of ACIP comprises of a Steering Group: Co-chaired by the CAD and MAS, this group identifies key money laundering (ML), terrorism financing (TF), and proliferation financing (PF) risks. It comprises eight banks, the Association of Banks in Singapore (ABS), and other relevant industry participants as well as Expert Working Groups (WG's) or Operational Task Forces: The Steering Group forms these groups to delve deeper into specific risk areas and develop strategies to address them. These groups include industry experts from various financial sub-sectors, legal and accounting professionals, and company service providers. Their diverse expertise helps ACIP develop a comprehensive approach to combating financial crime.

- **Anti Scam Command & Anti Scam Centre (ASC):** The Singapore Police Force (SPF) established the Anti-Scam Command (ASC) in 2022[76] to consolidate expertise and resources including the Anti Scam Centre. This involved integrating scam investigation, incident response, intervention, enforcement, and sense-making capabilities under a single umbrella. The command comprises the Anti Scam Centre, three Investigation branches and oversees the Scam Strike Teams situated within each of the seven Singapore Police Land Divisions. The ASC is part of the Commercial Affairs Department, which also houses the country's Financial Intelligence Unit and white-collar crime forces. One of the primary functions of the ASC is to carry out proactive online surveillance, identifying likely scam situations, for example, they use tools and analytics to detect and block scam websites, and thereafter providing warnings to potential scam victims. The ASC partners with more than 80 institutions in the fight against scams. These include local and foreign banks, card security groups, non-bank FI's (e.g., Grab, Singtel, DASH), Fintech companies and cryptocurrency houses (e.g., Wise, Xfers Pte Ltd and Coinhako), and remittance service providers in Singapore. In addition, the Government Technology Agency has deployed staff at the ASC to support Police investigations in scams related to SingPass. This facilitates faster sharing of information required for investigations and enables the SPF to leverage SingPass' fraud analytics capabilities that identify and flag unusual account activities. Getting to this stage and making it work since required co operation, for example:

  - The Singapore Police and DBS join forces to combat scams in October 2019. The Association of Banks in Singapore established an Anti-Scam Taskforce in 2020, which was later superseded by the ABS Standing Committee on Fraud in 2022[77].

  - The Anti-Scam Centre expanded to include a small group of employees from six leading banks in Singapore in September 2022[78], who agreed to co-locate some staff into the ASC to help the police tackle scam incidents efficiently. Employees from DBS Bank, OCBC, UOB, Standard Chartered, HSBC, and CIMB have been helping to trace the flow of funds, and freezing bank accounts involved in scammers' operations, as speed is important to tackle scams.

  - In 2023[79], through the work of Singapore's Anti Scam Centre (ASC), more than 19,600 bank accounts were frozen following reports made to it, and ASC helped recover more than $100 million. Working with foreign law enforcement partners, 19 scam syndicates targeting Singapore victims from their operations overseas were dismantled. These included 6 fake friend call scam syndicates and 3 phishing scam syndicates. More than 110 individuals based overseas, who were responsible for more than 730 scam cases, were arrested in these operations.

- In a targeted campaign over 15 weeks (September - December 2023[80]), the ASC & 4 of the Banks were able to prevent more than 15,000 scam victims from losing over $69.43 million, by using robotic process automation (RPA) technology to identify job, investment, and other scam victims. RPA uses bots or artificial intelligence to learn and then replicate repetitive tasks.

- From Sept 16 to Dec 31, 2023[81], the police and the banks issued more than 48,000 SMS's to the victims, who are customers of the four banks, interrupting over 5,300 scams in progress. The efficiency (speed) improvements that the ASC has been able to generate are significant and speed in scam cases is crucial. For example, working together, Singapore has seen a significant reduction in the average number of working days required to retrieve bank account holders' details and bank statements. Before the collaboration, it took 14-60 working days to retrieve bank account holders' details and bank statements. With the ASC's involvement, the process has been streamlined: 1 working day to freeze bank accounts, 3 working days to screen for bank account holder details & latest bank balance & 5 working days to retrieve bank statements.

- In 2023[82], the ASC successfully conducted more than 590 interventions, further averting more than $44 million of potential losses for these victims. In 2023[83], SPF worked with local Internet Service Providers to block over 25,000 scam websites. In addition, under Project ASTRO, by automating alerts from ASC to 28,541 potential at-risk citizens, notifications prevented S$148.7 million from being lost to scammers and was safeguarded, with 28,541 victims alerted.

- **Scam Awareness:** Singapore launched a **National Campaign**: The "I Can ACT Against SCAMS" campaign on 18 Jan 2023[84] to educate the public on scam prevention. Reminding Singaporeans to ADD (Hardware, Software and Security Settings), CHECK (Taking time to spot scam signs, checking with trusted others, and reconsidering decisions and action before sharing any money or private information) and TELL (Informing Authorities and communities about scam encounters, signs and trends. The Singapore Government announced in February 2024 that it "*will further boost our public education efforts by consolidating anti-scam resources into a one-stop portal on scams this year. (a) The website will include information on what you should do if you think you have fallen prey to a scam, how you can protect yourself, as well as the latest scam trends. (b) It will also provide information on where victims of scams can seek support*". Additional initiatives include:

    - **Targeted Messaging:** Project TEMPESTE disseminates targeted messages to inform the public about various scam types and prevention methods.

    - **Community Involvement:** The Anti-Scam Command participates in dialogues and webinars to foster community trust and inclusiveness in the digital space.

    - **ScamShield:** The ScamShield[85] app, a Singapore innovation launched in November 2020 and sponsored by the government, can be downloaded to mobile phones in Singapore. ScamShield blocks incoming calls from scammers and scans SMS's received from unsaved contacts to detect scam SMS's. It also allows users to report scam messages and calls. ScamShield actively filters scam messages and calls from numbers used in illegal activities, significantly reducing the likelihood of people being contacted by scammers.

    - **Scam Alert Website:** The National Crime Prevention Council (NCPC) established a Scam Alert website[86] to combat scams and cybercrime. The site focuses on promoting public awareness on crime and propagating self-help in crime prevention. The site includes weekly scam updates and details about the most prevalent scams affecting Singapore.

    - **Resources:** IMDA's "Digital for Life" Training Resources were published in January 2024[87] to encourage Singaporeans of all ages and backgrounds to embrace digital learning as a lifelong pursuit.

- **One Stop Government Portal:** The Singapore Government announced in February 2024[88] that it will further boost public education efforts by consolidating anti-scam resources into a one-stop portal on scams this year. The website will include information on what you should do if you think you have fallen prey to a scam, how you can protect yourself, as well as the latest scam trends. It will also provide information on where victims of scams can seek support.

- **Engagement Initiatives:** Outreach efforts include public education sessions, media interviews, and school talks to raise awareness. Over 141 sessions were organised in 2023, involving over 237 hours and reaching an audience of 40,835.

- **Banks and Other FI's:** Scams typically target the funds of victims, either by accessing compromised accounts, using stolen cards, or deceiving victims into transferring funds directly. Banks and FIs are at the forefront of this battle. The MAS mandates that they secure digital systems. This includes implementing multi-factor authentication to verify a customer's identity and authorising online transactions, as well as sending notification alerts to customers for reporting unauthorised transactions promptly. However, it is important to note that scammers can still circumvent these digital security measures by tricking customers into inadvertently revealing their account access credentials or downloading malware, thus gaining total or remote access to victims' devices and accounts. Singapore Banks and FI's are on a journey to design and implement effective and sustainable anti scam programmes, recognising few countries Banks' and FI's have yet achieved close to maturity, effectiveness or sustainability in this area and doing so will take quite some time. Nevertheless, benchmarking current Anti Scam Programmes to best practices provides Banks and FI's with opportunities to identify and close any gaps particularly where inherent risks are high and controls are not yet effectively mitigating these risks. For more details on what best practice anti-fraud programmes for Banks/FIs may look like, contact the GCFFC secretariat, which has collated a best practice guide. Key actions and initiatives relating to Singapore Banks & FIs are also included under regulatory supervision below.

- **Regulatory Supervision:** The Monetary Authority of Singapore (MAS), the financial regulator has also increased its focus on scams and how the financial services sector they regulate can respond. The main initiatives are as follows:

  - **MAS Technology Risk Management Guidelines:** In January 2021[89], the MAS required banks and FIs to secure digital systems. This includes implementing multi-factor authentication to verify a customer's identity and authorise online transactions, as well as sending notification alerts to customers so they can report unauthorised transactions promptly. However, it is important to note that scammers can still bypass these digital security measures by deceiving customers into inadvertently divulging their account access credentials or downloading malware, thereby granting scammers total, or remote, access to victims' devices and accounts.

  - **MAS & ABS announce measures to bolster digital banking security:** In January 2022[90], the MAS announced expectations that all banks and FIs to have robust measures in place to prevent and detect scams, as well as effective incident handling and customer service in the event of a scam. "The growing threat of online phishing scams calls for immediate steps to strengthen controls, while longer-term preventive measures are being evaluated for implementation in the coming months," MAS communicated in January 2022[91], Mr. Ravi Menon, then Managing Director of MAS, stated, *"MAS is deeply concerned about the recent spate of scams and the financial losses suffered by victims. The threat of scams will not go away, but we can reduce our vulnerabilities. This requires a multi-pronged response across the ecosystem. MAS, together with the Police, IMDA, and other relevant government agencies, is working closely with the financial industry, the telco industry, consumer groups, and other stakeholders to strengthen our collective resilience against scam attacks. We will ensure that digital banking remains secure, efficient, and trusted*".

  - **Additional Measures to Strengthen the Security of Digital Banking announced by the MAS & the ABS.** In June 2022[92], the MAS & Association of Banks in Singapore (ABS) announced additional measures to further safeguard customers from digital banking scams. These measures complement those announced earlier.

- **Banks introduce self-service Kill Switch for customers:** In October 2022[93], Singapore Banks have provided users with a self-service emergency "kill-switch" to suspend any compromised bank accounts

- **Banks introduce new "Money Lock" feature for customers:** In November 2023[94], Singaporean Banks introduced a new "Money Lock" feature, for customers to set aside an amount that cannot be digitally transferred or used. At the same time, the CPF Board introduced a default daily limit of $2,000 for online CPF withdrawals, which cannot be increased without strong authentication. Members also have the option to reduce this limit to $0, to disable all online withdrawals.

- **ABS Standing Committee on Fraud:** In 2022[95], the Standing Committee on Fraud (SCF) succeeded the ABS Anti Scam Taskforce established in 2020 (see above). The SCF aligns the banking sector perspective on whole-of-Singapore initiatives to address the rising occurrence of digital scams. The SCF, working with the MAS & SPF, coordinates the industry's continuous anti-scam efforts to implement robust practices that safeguard customers, so that they may continue to enjoy the benefits of digital banking with confidence in its security. The SCF comprises senior representatives from the seven Domestic Systemically Important Banks, and will develop and drive industry strategies for combating scams: including Monitoring and identifying potential weaknesses and opportunities with a view to develop and implement measures to combat digital scams; Promote sharing of best practices among banks on ever-evolving scam typologies and digital security trends; Providing industry-level guidance on implementation and enhancement of digital security controls across member banks; Heightening digital security awareness and good cyber hygiene among customers; Fostering inter-organisational and cross-sectorial collaboration with regulators and key government agencies to strengthen the ecosystem; Strengthening fund recovery efforts through enhanced cooperation among banks, SPF and other relevant stakeholders and achieving an equitable apportionment of losses among key stakeholders.

- **Collaborative Sharing of ML/TF Information & Cases (COSMIC):** COSMIC was launched on 1st April 2024[96]. COSMIC was co-developed by MAS and six major commercial banks in Singapore - DBS, OCBC, UOB, Citibank, HSBC and Standard Chartered Bank. COSMIC, which stands for ..is the first centralised digital platform to facilitate sharing of customer information among Banks & FI's to combat money laundering terrorism financing and proliferation financing globally. The Financial Services and Markets (Amendment) Act 2023 and accompanying subsidiary legislation, set out the legal basis and safeguards for such sharing. Ms Loo Siew Yee, Assistant Managing Director (Policy, Payments & Financial Crime), MAS, said, "*COSMIC will enable FIs to warn each other of suspicious activities and make more informed risk assessments on a timely basis. It complements the industry's existing close collaboration with MAS and law enforcement authorities to combat financial crime. This will strengthen Singapore's capabilities to uphold our reputation as a well-regulated and trusted financial centre.*"

- **Professional Digital Enablers:** Singapore passed the new **Online Criminal Harms Act** in July 2023[97], which sets out ex-ante requirements that online platforms must adopt, to better protect their consumers. The Act empowers the government in certain circumstances to order the removal of websites and online accounts that are suspected of being used for such purposes, thereby proactively disrupting scams and malicious cyber activities before more damage is done and more victims are involved. The Bill also provides for penalties ranging from fines to imprisonment, and in some cases, caning, for offenders who fail to comply with the removal orders or who obstruct enforcement actions. The Act also provides for the government to name and designate particular digital businesses which then makes them subject to codes of practice and implementation directions. The Singapore government has indicated that it will adopt a collaborative and consultative approach when formulating codes of practice, and digital businesses should make use of all opportunities to have their voices heard and interests protected. A number of important E Commerce initiatives have been taken in Singapore including as follows:

  - **Singapore E-commerce Marketplace Transaction Safety Ratings & Updated Guidance:** In May 2023[98] and in order to secure e-commerce marketplaces from scams, the Singapore Inter-Ministry Committee on Scams (IMCS) published E-commerce Marketplace Transaction Safety Ratings (TSR) to provide consumers with information on anti-scam measures that major e-commerce marketplaces have in place. Facebook Marketplace received the lowest ratings. The TSR will be published annually going forward. The IMCS also published revised Guidelines for Electronic Commerce Transactions (TR 76) to

provide e-retailers and online intermediaries such as e-commerce marketplaces, with additional guidelines to better secure e-commerce transactions from scams. The additional anti-scam guidelines set out best practices for e-retailers and e-commerce marketplaces. These best practices secure different areas of transactions, covering pre, during, and post-purchase activities, customer support, and merchant verification. The intent is to better enable merchant authenticity, improve transaction security, and aid enforcement against e-commerce scams. The additional guidelines are part of the safety features rated in the TSR. Generally, e-commerce marketplaces that adopt the guidelines would score better on the TSR. Sun Xueling, Minister of State for the Ministry of Home Affairs and Ministry of Social and Family Development, emphasised the need for digital enablers to intensify their efforts in a speech to Parliament in February 2024[99]. She noted that measures to block scam calls and SMSes were implemented, but scammers shifted their tactics to social media and messaging apps. Meta products, particularly Facebook, WhatsApp, and Instagram, were implicated in nearly half of all scam cases in 2023, contributing to approximately 43% of the losses, amounting to around $280 million. She commended platforms like Shopee and Carousell for their cooperation with the Ministry of Home Affairs (MHA) and the Police, citing Shopee's introduction of seller verification features in December 2022, which led to a 71% reduction in e-commerce scams reported on their platform between 2021 and 2023. Conversely, Meta has been resistant to implementing recommended safeguards on Facebook, despite the platform accounting for nearly 50% of e-commerce scam cases in 2023. As a result, Facebook Marketplace received the lowest ranking in the MHA's E-commerce Marketplace Transaction Safety Ratings (TSR) for the second consecutive year.

- **ASC Collaboration with Google to tackle malicious malware:** In July 2023[100], the ASC announced a collaboration with technology companies to flag and block malicious URLs, with the SPF enrolled into the newly launched Google Cloud Priority Flagger Program. This program aims to accelerate the identification and flagging of potential phishing websites and malware hosted on the service. By being a priority flagger, SPF's submission of the malicious websites and malware will be prioritised by Google for their action. SPF has also been working with online platforms, including Google, to introduce stronger safeguards to mitigate the risk of fraudulent takeover of online messaging accounts, such as through the pre-emptive detection and blocking of URLs linked to phishing sites. SPF uses analytic tools to identify and block scam websites.

- **Centre for Advanced Technologies in Online Safety:** In January, 2024[101], a new centre focused on building tools to detect harmful online content is to be launched under a S$20 million research initiative to grow Singapore's capabilities at combatting online harms, including misinformation and content manipulation. The research programme, dubbed the Online Trust and Safety Research Programme, runs from 2023 to 2028, and will be led by the Ministry of Communications and Information. A Centre for Advanced Technologies in Online Safety will be established under this initiative and will focus on building tools that will detect harmful content such as deepfakes and non-factual claims, for example, and identify societal vulnerabilities. It also aims to develop possible interventions to reduce online users' susceptibility to harmful content. It will bring together companies and technologies to increase the ability to create a safer internet. The goal is to detect fake claims and dangerous deepfakes. These research efforts will also help develop new technologies needed to protect against harmful information and misuse on the internet.

- **Telco's:** The telecommunications sector in Singapore plays a crucial role in combating scams and is regulated by the Infocomm Media Development Authority (IMDA). Telecommunication companies collaborate with the government and other industry partners to block or filter scam calls, messages, or websites. They employ technologies such as caller ID spoofing detection and spam filtering to prevent scams. Additionally, they work with the government to restrict access to websites associated with scams and educate customers on recognising and reporting scam-related activities. IMDA requirements on Singapore Telco's helped to block a total of more than 310 million potential scam calls in 2023. The volume of international calls attempting to spoof local numbers also declined significantly, from 706 million in 2022 to 18 million in 2023. Particular actions include the following:

- **Singapore Telcos block scam calls:** In 2019[102], The Infocomm Media Development Authority (IMDA) has been enhancing safeguards against scam calls since 2019, requiring Singapore Telcos to block calls from known scam numbers.

- **Singapore Telcos block robocalls:** In 2020[103], IMDA has continued to impose additional requirements on Singapore Telcos to block robocalls, using pattern recognition technology.

- **Singapore Telco's blocking spoofed numbers and SMS with malicious links (to End 2022):** In 2022[104], the Infocomm Media Development Authority (IMDA) continued to add further requirements on Singapore Telcos blocking spoofed local numbers & SMSes containing malicious content and links

- **Registration Requirements for SMS Sender ID's:** In January 2023[105], Singapore made it mandatory to register all alphanumeric SMS sender IDs with the Singapore SMS Sender ID Registry (SSIR). This helps to prevent spoofing of legitimate sender IDs registered with the SSIR, and to ensure that messages from unregistered sender IDs are labelled as "Likely-SCAM". Cases involving scam SMSes fell by 70% over three months, after mandating the SSIR.

- **International Co operation:** In 2023[106], Singapore hosted the inaugural Regional Anti-Scam Conference, attended by representatives from 15 countries. Sun Xueling, Minister of State for the Ministry of Home Affairs and Ministry of Social and Family Development, emphasised the necessity of international cooperation to combat fraud, citing the more than $55 billion lost worldwide to scams in 2021 and the ease with which these schemes cross borders. The Minister underscored the importance of funds recovery, establishing international norms, and sharing information on criminal typologies and effective strategies to enhance the global fight against scams. On 12 March 2024[107], a first of a kind Global Anti Fraud Summit was held in London, U.K., attended by G7 countries, as well as South Korea, New Zealand & Singapore which issued a communique promising further international co operation and collaboration. Hong Kong was not in attendance.

9.6 Overall KPI's on Prevention & Recovery Etc

Singapore has not published targets but it does report annually through the Police Force on Scams. It also tracks and reports Scam related KPI's provided by the Singapore Scam Management System (SMS)[108]:

- **Total Amount Recovered:** The Anti-Scam Centre has successfully recovered a total of S$410.9 million

- **Bank Account Interventions:** Over 60,600 bank accounts have been frozen, aiding recovery of funds.

- **Telecommunication Actions:** More than 20,400 mobile lines have been terminated, and over 83,400 WhatsApp accounts reported.

- **Online Marketplace Measures:** Removal of over 11,500 suspicious online monikers and advertisements.

9.7 Liability & Reimbursement

The Singapore Government's stance on liability and reimbursement was articulated in Parliament by the Minister of State for Trade and Industry Alvin Tan in September 2023[109]. The Minister stated: "*There are perspectives that banks can effortlessly absorb losses from individual scam cases. However, providing full restitution without due consideration of culpability is neither equitable nor advisable. Such an approach can diminish vigilance and personal responsibility, leading to user complacency. Ms Sylvia Lim proposed that customers depend on banks to ensure the security and robustness of their online banking and payment systems. This is indeed the case. The MAS mandates banks to secure digital systems, including implementing multi-factor authentication to verify a customer's identity and authorise online transactions, and sending notification alerts to customers so they can promptly report unauthorised transactions. However, it should be noted that scammers can still circumvent these digital security measures by tricking customers into unintentionally revealing their account access credentials or downloading malware, thereby granting scammers complete access, or remote access, to victims' devices and their accounts. Individual customers*

thus have a crucial responsibility to protect access to their accounts, which includes practising good cyber hygiene and being diligent in preventing their login information and OTPs from being disclosed to third parties. MAS has issued guidelines for banks to establish clear customer handling and investigation processes and to treat customers fairly in all disputes. MAS also oversees how banks manage such disputes. In scam cases, banks must consider if they have fulfilled their obligations, and whether the victim had acted responsibly. Customers who practised good cyber hygiene and were diligent in preventing their login information and OTPs from being disclosed to third parties should not bear losses. Depending on the specifics of each case, banks may offer goodwill payments to customers. If a customer is unsatisfied with an offer, he may decline and approach the Financial Industry Disputes Resolution Centre (FIDReC) for mediation and adjudication. A customer can further pursue his case in court if he is not satisfied with the outcome. If the customer accepts a goodwill payment offer, he or she will be bound by the terms of the offer. Should new information emerge that is materially different from the premise upon which the customer had accepted the goodwill offer, the customer can request the bank to relook the case, or approach FIDReC for assistance."

Shared Responsibility Framework: In October 2023, the MAS and IMDA published a consultation paper on the proposed Shared Responsibility Framework (SRF)[110] which is currently limited to phishing scams. The SRF outlines a collaborative approach to distribute the burden of losses from phishing scams losses across FIs, telecommunication operators (Telcos), and consumers. This pertains to unauthorised transactions that result from such scams. The framework's objective is to expedite the process for consumer redress, while also encouraging vigilance within the financial ecosystem. It specifically calls for FI's and Telcos to adopt robust anti-scam measures and to proactively educate consumers on scams prevention. However, it does not yet address losses stemming from malware or scams where authorisation was given. Under the SRF, if there is a failure to adhere to prescribed duties, Banks/FI's are initially held responsible and will bear the entirety of the incurred losses. Conversely, if an FI has met all its obligations and a Telco is found to have failed in its responsibilities, then the Telco will be expected to absorb the full losses. Liability for the Telco arises solely if the phishing scam was executed through SMS. Should both the FI and Telco have fulfilled their respective duties, the consumer would then assume responsibility for all the losses.

9.8 Singapore Scam Response Risk Assessment Dashboard - In more detail

Singapore has acknowledged the severity of scams-related threats. Although significant strides have been made, the nation understands that continued efforts and effective initiatives are essential to combat this

Key Findings & Possible Actions
Focus Areas - 10 Categories

For Consultation

1. International Leadership
2. National Leadership and Co Ordination
3. Policing & Law Enforcement
4. Finance Including Payments
5. Higher Risk Technology & Digital Businesses
6. Information, Intelligence Sharing & Information Security
7. Education & Awareness
8. Technology & Innovation
9. Losses
10. Victims

ongoing issue. For more details on Singapore's response see the response risk assessment Dashboard below: 9.8 Singapore Scam Response Risk Assessment Dashboard - In more detail

Response including Cross Sector Contributions - Government, LEA, Finance & Digital Enablers - Singapore 🇸🇬			
Response	**Higher Level of Response**	**Moderate Level of Response**	**Lower Level of Response**
1. Government			
1.1 Anti Fraud Strategy	Singapore is prioritising tacking fraud and scams including for National Anti Scam Command & Centre (NASC) opened in 2022	N/A	N/A
1.2 Lead Anti Fraud Agency	Singapore Police Force - Commercial Affairs Department	N/A	N/A
1.3 Government Targets	N/A	N/A	No Specific Targets Set
1.4	SPF Annual Scams & Cybercrime Brief & biweekly via "Scamwatch"	N/A	N/A
1.5 Awareness Campaign's	"I can ACT against scams" campaign launched in January 2023	N/A	N/A
1.6 PPP Collaboration (E.g. Anti Scam Centre/ Private to Private)	National Anti Scam Centre opened 2022 with 6 Banks co located & other Organisations involved	N/A	N/A
2. Police & Law Enforcement			
1.7 Policing Priority to tackle scams	National Anti Scam Command established by SPF - Dedicated Tools and Teams - Increased Focus and Attention	Data not available	Data not available
1.8 Clean up rates	Data not available	Data not available	Data not available
1.9 Victim Loss Recovery - LEA (est by GASA on average globally - 7%)	Data not available	Estimated by GASA at 9%	Data not available
3. Finance including Banks and FI's / Telco's			
1.10 FI Anti Fraud Programme (Clarity on AFP obligations/status)	MAS Announced Additional Measures required for Bank/FIs in 2021 & 2022	N/A	N/A
1.11 FI Prevention Rates	S$69.43M prevented by Banks in ASC (Sept - Dec 2023) - approx 30%	N/A	N/A
1.12 Reimbursement Rates	N/A	N/A	Proposed sharing framework FI/Telcos for phishing loss only - Consultation
1.13 Awareness Campaigns	All major Banks regularly educate and make customers aware of Scams	N/A	N/A
1.14 Telco's	IMDA requirements on SG Telco's include on SMS, robo calls - spoofing etc helped to block 310 mio potential scam calls in 2023	N/A	N/A
4. Digital Enablers and Businesses			
1.15 Codes of Conduct/ Robust Anti Fraud Programmes	N/A	Online Criminal Harms Act 2023 empowers SG Gov to to instruct e.g. websites to take down materials etc	N/A

9.9 Key Findings & Recommendations

This assessment of Singapore, together with assessments of Australia & Hong Kong have generated insights which have been translated into possible findings and actions that will be consulted on as set out in Section 10 below.

10. Key Interim Findings & Possible Actions - For Consultation

Tackling scams is no longer an option with scam crime rates at pandemic levels across the world and not just targeting Australian, Hong Kong and Singapore's citizens. Any response requires collective effort, from both state and citizen, from policing to education, from finance to telecommunications and technology to e commerce and social media, both domestically and internationally. It also needs a focussed smart response taking up the most important actions that will make the most difference.

Each of Australia, Hong Kong and Singapore have recognised that tackling scams requires a multi year collective effort, from both state and citizen, from policing to education, from finance to telecommunications and technology to e commerce and social media, both domestically and internationally.

Based on the research carried out into the Australia, Hong Kong and Singapore countries and summarised in this paper, the GCFFC APAC Chapter believe the following may have merit and is consulting on which of the actions highlighted below may make an important difference and be supported going forward to improve the effectiveness in fighting scams.

10.1 Brief Summary of Responses and Possible Actions - In Consultation

The main focus for responses, include more international co operation, stronger, more coordinated and effective national leadership and co ordination across all sectors, law enforcement prioritising anti scam centres, finance sector prioritising measures to target unauthorised scams and increasingly measures to tackle authorised scams which have been introduced elsewhere and can be assessed for effectiveness, other private sector measures, particularly as most scams today originate through technology and digital businesses' products and services, private sector collaboration, education and awareness, use of and defences against new technology, and responses to losses and victims. Picking just a few key actions as highlights would be:

- An **international response** to support common decisive actions to tackle scams.

- Urgent International action to help the estimated 500,000 kidnapped **modern slavery/human trafficking** victims mostly in South East Asia forced into scam criminality and incentivised to co operate through extreme brutality.

- Establishing **National Anti Scam Centres**, with Singapore an example of public and private collaboration including co locating Banks and other private sector actors contributing. Creating an accurate and updated list of scam perpetrators, including names and or other potentially identifying information, including accounts used and shared with Banks & Payment Service Providers in order to block likely related scam transactions.

- Ensuring **Banks and other FI's deploy reasonable anti scam programmes**, which manage scam risk and customer satisfaction to an appropriate extent. Supervisory leadership is essential, with genuine consultation with the industry to determine the most effective measures crucial. Both the HKMA and the MAS have introduced requirements on their sectors to tackle scams, following substantive engagement with the sector to determine appropriate necessary actions. ASIC in Australia carried out a Scams review sharing its findings on the Big 4 Banks in 2023, which identified difference and laid out expectations. Efforts have increased by FI's over the following year to tackle scams, issue warnings, self service and to introduce positive friction which is or has been contrary to other supervisory policy objectives related to faster, cheaper payments and more open banking. Compromises will need to be made to adjust to find a balance. The GCFFC APAC Chapter is working with Banks and FI's to suggest areas where best practices can be shared to improve the effectiveness of Bank/FI anti scam programmes.

- Enacting **new laws and regulations to give authorities powers to act against telco, technology and digital businesses that facilitate scams** through the abuse of their products and services, where responses to date are in many cases insufficient. The GCFFC APAC Chapter have developed areas where telco, technology and digital businesses could do more. Singapore has enacted a new law, Australia is consulting on Industry codes.

- **Information Sharing** capabilities, with Hong Kong's FINEST, an example where Banks and FI's in Hong Kong can share information on corporate accounts with one another through the Financial Intelligence Evaluation Sharing tool ("FINEST") launched in June 2023. A current HKMA proposal out for consultation points out that FINEST's ability to prevent and detect crime would be enhanced if information sharing were extended to personal accounts because a significant portion of mule account networks involve bank accounts held by individuals. The GCFFC APAC Chapter have responded to this consultation supporting an extension of information sharing to include scams involving bank accounts held by individuals.

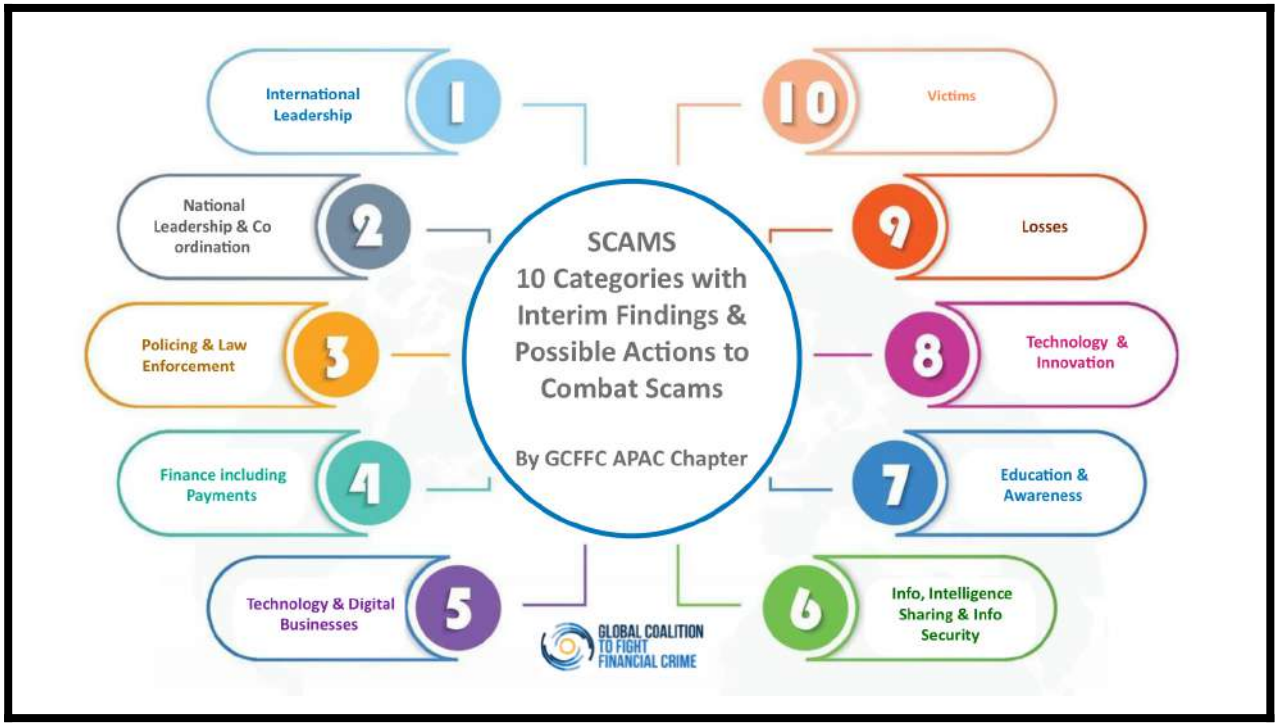
- **Technology - Artificial Intelligence** is both an enabler of scams as well as a necessary tool in response to tackle it. An arms race is underway between those exploiting technology and deploying tools that have nefarious and or even dual use purposes such as mass marketing, deep fake technology etc with those defending data pools, customer credentials and customer assets. The volume of attempted scams today means that large firms be they Banks FI's, Telco's, Technology or other Digital Businesses are faced with a significant volume of data too large for individual human intervention or immediate analysis to be viable. However, this data can be supervised as Artificial Intelligence through machine learning can be trained to identify potential fraud scenarios using multiple data points, providing a much richer lens on potential criminality being perpetrated by or against customers. This in turn enables more precise customer interventions and ensures models learn faster to keep pace with criminals who continually adapt their attack methods, surfacing suspect scam activity earlier or even before it happens. The accumulation of clean useful data across industries and the acceleration of AI deployment to this data to detect and prevent scams is underway but needs greater support.

- **Incentives** - Law enforcement action to recover funds or take down scam criminal gangs rely on international co operation which can be limited and often not straightforward once funds leave a victims jurisdiction. Countries with high levels of scam losses and cases could consider establishing whistleblower programmes to incentivise even scammers themselves to provide intelligence and information about their associates to both gain information to target and to undermine the scammer community.

- **Losses** - Prevention must be the priority ahead of post loss liability or loss sharing models. Pre fixing liability, without considering case by case actions may appear attractive to some, but may also generate unintended consequences, which should be considered and factored in before any decision is taken to proceed in this direction. For example generous third party compensation models will encourage first party fraud, and dis-incentivise potential future victims in becoming scam aware, generating ever more illicit proceeds for the scammers. As a counter, third parties made responsible are likely to improve their own defences to prevent and mitigate scam losses but are just as likely to increase friction through restricting access to related products and services, and these may adversely affect vulnerable victims the most. Careful consideration of costs and benefits should be assessed and fairness should be included before any new models are introduced.

- **Victims -** Victims, especially the vulnerable should be supported and treated as such and provided with necessary support to deal with the crime committed against them and the consequences from their experiences, recognising their will never be a guarantee of full justice or full compensation In all cases.

10.2 In More Detail For CONSULTATION



1 - International Leadership: Currently there is no international body established or mandated to lead the international fight against financial scams. This could be the FATF, but this would require an extension and material change to its mandate, and its workload. It has recently rejected this route, though supports alternative international leadership in this space. The UK has held a first international ministerial summit with G7 countries represented, plus Australia, South Korea and Singapore. This suggest this is the start of an opportunity which should be taken to work towards creating a new international organisation with a clear anti fraud and scams mandate, or a Fraud/ Scam Action Task Force.

The deficit in leadership is also a function of the lack of an internationally agreed instrument on fraud and or cybercrime despite a 4 year attempt to agree a Cybercrime Convention at the United Nations. Agreement broke down in February 2024, on fundamental grounds which will make resolving the differences around human rights challenging, but in any event the draft Convention must strive to go further than dealing with international law enforcement cooperation and instead needs to recognise that this is a more complex challenge & requires many more stakeholders that are required to be involved in combatting cyber enabled financial scams, by establishing comprehensive international standards & a body to oversee & monitor country implementation.

Possible Actions:

1.1 FATF to review whether it takes the leadership on scams and if not raises the gap as material with G7/G20 Ministers.

1.2 In the absence of FATF taking the lead, a new International Task Force be established to combat scams.

1.3 A UN Cybercrime Convention is needed, focusing on fraud and scams. Alternatively, add an additional protocol to the Palermo Organised Crime Convention to focus on fraud and scams,

including those facilitated by cyber means, as predicates for money laundering. It is essential that increased international law enforcement co operation is enabled. An international task force could be established off the back of the Convention.

1.4 Modern Slavery/Human Trafficking: Urgent international action is needed to rescue the estimated 500,000 victims of modern slavery/human trafficking used for Romance Baiting/Pig Butchering scams predominantly in South East Asia but also elsewhere, where treatment can be brutal and life threatening. If these victims were for example, American, European, Australian, Japanese or Singapore citizens kidnapped as tourists in South East Asia, instead of poor job seekers lured by fake job offers and then kidnapped and beaten to constantly work scams, this would not be tolerated. Those on the front line, such as NGO's who are often the only source of independent help need urgent support including significant financial resources to carry on and respond to the growing need for help and assistance to get survivors to safety. These very NGO's could also be a valuable source of data to support law enforcement and anti scam responses from Banks and other private sector bodies.

2 - National Leadership & Co Ordination: Countries should consider whether they should carry out a National Anti Scams Risk Assessment and from this determine a National Counter Scam Strategy, focussing on cyber enabled fraud and scams, where strategies to improve prevention is likely to be the central feature & targets should include reducing the incidence and harms from financial fraud & scams. If the overall risk rating warrants it, countries could consider appointing an Anti Scams Champion from a senior governmental position and or appropriate senior government leadership to tackle the overall response to financial fraud & scams, including identifying additional sectors that need to contribute and to ensure targets are set and measured and annual reporting on fraud threats and responses are published. A "whole of government/society" approach is likely to fare best with numerous agencies involved and working together also bringing together other non-governmental sectors including the private sector. Governments should look closely at vulnerabilities in their payment systems which can be exploited by scammers and fraudsters. Payment speed should be accompanied by appropriate authorisations and confirmations to protect payers. Criminal Codes should be reviewed to ensure that they capture activities perpetrated via new technologies (e.g. deep fakes).

Possible Actions:

2.1 Countries to carry out a National Anti Fraud and Scam Risk Assessment. The risk Assessment should inform a National Anti Fraud and Scam Strategy.

2.2 Countries should appoint and empower an Anti Fraud and Scam Champion in Government as well as identifying the law enforcement country lead and responsibility for, including co ordinating the law enforcement response, including international law enforcement co operation.

2.3 Establish a public private partnership dedicated to responding to anti fraud and scams, which includes the ability to share important public and private information to prevent detection Report and take action against fraudster and scammers. Create an accurate and updated list of scam perpetrators, including names and or other potentially identifying information, including accounts used to be shared with Banks & Payment Service Providers in order to block likely related scam transactions.

2.4 Building on a national scams risk assessment (see National Anti Scams Risk Assessment), authorities should ensure vulnerabilities in payment systems and opportunities to strengthen Criminal Codes are addressed.

See also below additional possible actions that may be included in a Countries overall National Anti Fraud & Scams Strategy, which will need to supported, if so by national leaders.

3 – Policing and Law Enforcement: Countries should consider how to ensure that Police and Law Enforcement skills and resources are fit for purpose and materially can contribute to fighting financial fraud & scams, including following the money and loss recovery, including through effective international cooperation. Elements of this could include establishing and leading National Anti Scam Centres, National Fraud Reporting Bureaus, and National Fraud Financial Intelligence Units, as well as working with the private sectors in such endeavours. Consideration could be given to establishing a dedicated "e or i anti scam investigation service", and or teams and or ensuring essential capabilities including certifications of skills are well established. Traditional policing methods may not be as successful or as appropriate in carrying out these tasks.

Possible Actions:

3.1 Law Enforcement leaders could consider reviewing law enforcement capabilities to assess their ability to match skills and resources with the threat from scams.

3.2 Law Enforcement leaders could consider whether there is merit in a new dedicated anti scams policing unit with specialist skills to investigate fraud and scams, and or certifying existing officers following appropriate training and learning.

3.3 Law Enforcement leaders could consider establishing i) an Anti Fraud and Scam centre, ii) an National Anti Fraud and Scams Reporting Office and or alternatively private sector reporting bodies, for example Crime Stoppers International, and iii) a National Anti Fraud & Scams FIU to assess reporting information and pass on to Law Enforcement for action.

3.4 Law enforcement action to recover funds or take down scam criminal gangs rely on international co operation which can be limited and often not straightforward once funds leave a victims jurisdiction. Countries with high levels of scam losses and cases could consider establishing whistleblower programmes to incentivise even scammers themselves to provide intelligence and information about their associates to both gain information to target and to undermine the scammer community.

4 – Finance including Payments: Banks and FI's should consider how to best respond to manage not only the threats from scams on their customers but also to themselves. Regulatory supervisors should also consider what level of response is required from Banks and other FI's, particularly those holding accounts and involved in payments.

Possible Actions:

4.1 Banks, FI's and Payment Service Providers (PSP's) could consider best practices in terms of anti scam programmes. For more details on these possible best practices a summary is available on

request from the GCFFC. This has been designed and developed in co operation with leading industry experts. Supervisors should prioritise anti fraud and scam actions by those they regulate, especially higher risk Banks and FI's (for fraud and scams) and include these in their supervisory plans.

4.2 Policy Makers could consider safe harbours for Banks, FI's and PSPs in taking action for example, in stopping suspicious payments, beyond instant payment cut off times, or other similar legitimate responses that also may affect innocent customers but require further investigation and or escalation.

4.3 Banks, FI's and PSP's could consider establishing their own private to private information sharing service, where legally permitted, and if not solicit the authorities to permit such sharing in order, for example to restrict repeat fraud and scammers from constant re offending using the same, similar or related and or connected credentials. Banks, FI's and PSP's should be prepared to support and contribute to the success in a countries dedicated Anti Fraud and Scam Centre (see 3.3 above).

5 – Higher Risk Technology & Digital Businesses: Countries should consider whether to place additional obligations on other relevant private sector companies in addition to Banks, FI's and PSP's, for example these are likely to include sectors such as the telecommunications (which may already be regulated), technology, and other digital businesses that enable fraud and scams, and in particular those in these sectors that represent higher risk of being used/abused for fraud and scams such as in search, mail, online retail/e commerce, gaming, dating, adult and social media including messaging etc. Many of these "Technology & Digital Businesses" currently fall outside direct regulation and act against scams on a purely voluntary basis. Voluntary action to date is considered by many to fall short in many cases of what is needed, as can be seen from the incidents and amounts of losses from scams year on year, facilitated through the products and services of many of these Technology and Digital Businesses. The move towards regulation has started already in a number of countries, for example as has been done in the UK in the Online Safety Act, in the EU in the Digital Services Act and in Singapore in the Online Criminal Harms Act.

For more details on what best practices for anti scams programme may involve for these private sector businesses, a best practices summary is available on request from the GCFFC secretariat. This has been designed and developed in co operation with leading industry experts.

Possible Actions:

5.1 As stated in 2.1 above, Countries could consider carrying out a National Anti Scam Risk Assessment, and in so doing identify the sectors that are particularly vulnerable and or facilitate the activity and consider what additional obligations these sectors should be subject. Those identified as highest risk, by sector, could be segmented using a threshold test which could be employed to catch for example only the largest facilitators (based on usage, turnover etc), and they could be required to take actions

5.2 Supervision responsibilities could be considered including which regulators would be appropriate.

5.3 Higher Risk Technology and Digital Businesses could consider supporting and contributing to the success in a countries dedicated Anti Fraud and Scam Centre's (see 3.3 above).

6 – Information, Intelligence Sharing AND information Security: Information and Intelligence sharing could be encouraged further and legally permitted with safeguards to both enable private to private, public to public and private to public and vice versa sharing for the purposes of fighting fraud and scams. Whilst these safeguards could include data protection, privacy is not a static concept and norms about privacy are evolving, especially with the use of the internet, with many preferring to trade privacy for convenience & speed already. Attitudes to privacy have arguably

already changed with many giving up names, e mails, IP addresses, & telephone details often just to get online at airports or train stations or in coffee shops. Whilst the sharing of information including identity information is prevalent online, including tracking through cookies, geolocation in mobile phones, and records of bank and payment details when purchasing goods and services, those that acquire this information will need robust data protection and information security programmes, to keep this data safe. For regulated businesses, being able to share information on known or suspected scammers is important, and will protect customers and could be considered. This may require legal and or regulatory changes and or support to enable effective information sharing, which is consistent with modern data protection principles.

Possible Actions:

6.1 Countries could consider whether legal gateways to information sharing could be provided to support necessary and proportionate sharing in order to tackle anti fraud and scams, in particular the sharing of suspected fraud and scam techniques and personal data about particular suspected and or higher risk fraudsters or scammers and related persons and entities. This could be done at least in a countries considering dedicated Anti Scam Centres (see 3.3 above).

7 – Education and Awareness: Citizen awareness and training materials can be created and deployed. Intelligence and information can be generated also from reports received and warnings provided through empowered agencies. Citizens have a vital role in the fight against scams and need to stay abreast in particular of online banking hygiene practices as scam tactics evolve. These include: keeping apprised of scam advisories and alerts put out, referring to official sources, such as those on regulators websites and or issued by banks, for hotline numbers and website addresses to communicate with banks, moving towards greater use of bank apps for banking needs and receiving notifications by turning on in-app notifications on their devices; never clicking on links provided in SMS's or emails unless sources are clearly and can trusted, never divulge internet banking credentials or passwords to anyone; verify SMS's or emails received by calling the bank directly on the hotline listed on its official website, verify that you are at the bank's official website before making any transactions, or transact through the bank's official mobile application; and closely monitor transaction notifications so that any unauthorised payments are reported as soon as possible to increase the chances of recovery.

Possible Actions:

7.1 Countries could commission regular awareness raising campaigns to make citizens and customers aware of the threat and the best responses and available resources to combat fraud and scams. Campaigns can ensure that victims understand the importance of reporting scam incidents. Empowering victims with the knowledge and resources to report scams may also be useful in holding perpetrators accountable and preventing future incidents. Providing awareness tools FIs can leverage in their own awareness campaigns can be powerful.

7.2 Regulated businesses could also use their channels to educate and raise awareness among their customers generally and when using their products and services.

7.3 Further tailored training could be offered for police, law enforcement and those in Banks, FI's & PSP's that are responsible for investigating fraud and scam cases.

8 - Technology & Innovation:

Technology powers the digital economy and the digital world and is both part of the problem as well as being an indispensable part of the solution and or response to tackling scams. With the 4th Industrial Revolution well underway and unstoppable, the benefits it provides are very significant and with the development of AI beyond machine learning for example also into generative AI, the prospects for further benefits for all can be imagined. The unintended consequences for these innovators, however has been to make it easier to commit scams and to do it at scale, faster, quicker, cheaper and with less risk, and the prospects of additional tools including AI-based applications, are likely to also benefit the fraudsters and scammers as well.

Technologies that can actively support criminality can be identified in a countries National Anti Scam Risk Assessment and higher risk technologies can be identified. Technologies, for example, that can create highly plausible 'deep fakes", such as manipulated or synthetic audio or visual media that are created to appear authentic, and which feature people that appear to say or do something they have never said or done, created using digital AI tools such as machine learning and deep learning, could be considered to be restricted, and or subject to licensing and or other control measures. Deep fakes are a subset of a broader category of AI generated synthetic media, which not only includes video and audio, but also photos and text. 3D animation technologies can also yield similar results.

Technologies that can actively support tackling criminality can also be identified and promoted. Banks, FI's and PSP's are on the front line in preventing customer losses and or money laundering and with huge volumes of attempted fraud and scams targeted at Bank customers, products and channels, technology solutions will need to keep pace to protect prevent and detect attempted fraud and scams as well as laundering the illicit funds from fraud and scam activities. The volume of attempted fraud means that firms are faced with a significant volume of data too large for individual human intervention or immediate analysis to be viable. However, this data can be used to the FI's advantage as AI through machine learning can be trained to identify potential fraud scenarios using multiple data points, providing a much richer lens on potential criminality being perpetrated by or against FI customers. This in turn enables more precise customer interventions and ensures models learn faster to keep pace with criminals who continually adapt their attack methods, surfacing suspect fraud or scam activity earlier or even before it happens. AI is already helping to keep customers from falling victim to fraud and scams by identifying likely patterns of activity or customer behaviour. For more details see the recent GCFFC "Frequently Asked Questions on the use of AI as a tool to accelerate effectiveness in fighting financial crime in the private sector for Financial Institutions" (insert link), which also included the following *"By using AI machine learning, and training it on mass data where fraudulent transactions and non fraudulent transactions are clearly identified, it can deploy multiple rules that can predict whether a particular transaction is likely to be fraudulent, is stopped and or is escalated for further review once a prediction becomes likely or reaches a particular threshold and as important continues to learn by being fed new data where fraudsters have evolved and used new techniques. It is impossible for humans to compete with machines when it comes to optimising thresholds over many criteria and combining these to generate a combined prediction as to fraudulent activity. The human input adds the most value by sourcing the data and providing an environment for the system*".

Other sectors such as the technology, telecommunications, and other digital businesses, particularly those that ought to become regulated (see 5 above) may need to invest and deploy

additional tools including technology to prevent, block, take down and report fraud and scam related activity, posts, mails, SMS, messages etc. They may also have to consider changing or evolving existing business models, as a last resort if other actions are insufficient.

Possible Actions:

8.1 Technologies that can actively support criminality can be identified and supported in a countries National Anti Fraud & Scam Risk Assessment and higher risk technologies can be identified.

8.2 Higher Risk Technologies, could be considered to be managed for example by applying restrictions, and or subject to licensing and or other control measures.

8.3 Anti Scams Technology can be supported and considered to be deployed by Banks, FI's and PSP's to prevent and detect scams targeting their customers and the use of their products and services, including the use of AI machine learning. For more details see the best practices available from the GCFFC secretariat.

8.4 Anti Scams Technology can be considered to be deployed by Digital Businesses to prevent and detect scams targeting their customers and the use of their products and services, including the use of AI machine learning. For more details see the best practices available from the GCFFC secretariat.

9 - Losses: There may be differences of opinion as to who is expected to be responsible for genuine scam losses where these cannot be recovered from the scammers. Of course the scammers should be targeted first by law enforcement to recover the funds stolen but thereafter, depending upon the circumstances and the actions taken, the victim and or third parties could be responsible to contribute in whole or in part in making up the losses. Apportioning liability, left to the law and the courts in many countries is a complex task, where so-called unauthorised fraud and scams and so called authorised fraud and scams may be seen differently but in each case the level of carelessness and or negligence of victims and others may need to be weighed. Whether truly vulnerable victims are considered as a special category is likely to add additional complexity.

Any alternative liability models, for example pre fixing liability, without considering case by case actions may appear attractive to some, but may also generate unintended consequences, which should be considered and factored in before any decision is taken to proceed in this direction. For example generous third party compensation models will encourage first party fraud, and dis-incentivise potential future victims in becoming fraud and scam aware, generating ever more illicit proceeds for the fraudsters and scammers. As a counter, third parties made responsible are likely to improve their own defences to prevent and mitigate scam losses but are just as likely to increase friction through restricting access to related products and services, and these may adversely affect vulnerable victims the most.

Insurance may be an alternative, where large but unlikely tail risk events, like those from significant losses from scams can be addressed and a new market, where risks can be apportioned more efficiently, and data on scams, awareness and response, can be used to assess and incentivise better online behaviours. Insurance markets though still have their own problems with first party fraud and moral hazard, but at least these are factored in to the operation of this market.

Annex 1 - Best Practices for Anti Scam Programmes for Banks/FI's

Annex 2 Best Practices for Anti Scam Programmes for Higher Risk Technology & Digital Businesses

Available from GCFFC Secretariat/APAC Chapter Secretariat for Regulated/Relevant Businesses

Possible Actions:

9.1 Countries could consider prioritising the prevention of scams first and then the recovery of stolen funds from scams as well as education and awareness programmes in order that citizens have the information they need to stay safe online and or from scams.

9.2 Countries could in particular prioritise genuinely vulnerable citizens in order to protect them and the availability of and access to essential products and services.

9.3 Banks, FI's and Professional Digital Enablers could risk assess their products and services in order to have risk adjusted anti scam programmes designed to mitigate the threats to their customers and users from scams.

9.4 Countries could consider their current legal and regulatory frameworks to clarify how these currently are believed to respond, and to determine appropriate guidance and or changes to achieve a fair and equitable liability model, factoring in unintended consequences with the aim to minimise proceeds of crime generation for fraudsters and scammers.

10 - Victims: Those suffering losses from scams, particularly those that have been manipulated and involved in so called authorised frauds may be re victimised again, and so actions to protect victims could be further considered. Specific attention needs to be paid to the vulnerable.

Possible Actions:

10.1 Law Enforcement could update their protocols & establish consistent best practices on fraud & scams to ensure only persons that are not true victims are pursued, investigated or prosecuted.

10.2 Banks, Fi's & PSP's could update their protocols and establish industry best practices on fraud & scams to ensure only persons that are not true victims are pursued, investigated & reported.

10.3 Banks, FI's and PSP's could consider their actions carefully including whether and how to close accounts or restricting access to relevant services for money mules, where the behaviour is considered as unwitting and not intentional.

10.4 Law Enforcement, Banks, FI's and PSP's could have the capabilities to be able to direct victims to support services provided by experienced agencies and or NPO's that are able to offer i) take down, remove or similar services, and or ii) relevant victim counselling and support, which may also include Mental Health Support and help to manage finances, which can be provided by establishing partnerships with Charities and Peer-Support Groups.

10.5 Victims are entitled to have their cases treated as confidential, unless and until a court hearing is held where a prosecution is underway as against the fraudster or scammer.

These materials are available to regulated Banks/FI's only. They can be obtained upon request from the GCFFC Secretariat / GCFFC APAC Chapter Secretariat by request.

Annexe 2 - Screenshots

These materials are available to appropriate and relevant parties only. They can be obtained upon request from the GCFFC Secretariat / GCFFC APAC Chapter Secretariat by request.

Endnotes:

[1] See: https://www.interpol.int/en/News-and-Events/News/2024/INTERPOL-Financial-Fraud-assessment-A-global-threat-boosted-by-technology

[2] See: https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/home

[3] See: https://www.bis.org/bcbs/publ/d558.pdf

[4] See: BIS highlight 2 main concerned for supervisors for financial stability related to scams being, *"financial losses to banks resulting from digital fraud, suffered by banks themselves directly (eg banks unknowingly sending funds to fraudulent counterparties) or due to the need to refund their clients (eg banks having to compensate customers for losses suffered – be it the banks' fault or not). In extreme cases, such financial losses could reduce banks' capital resources and shock- absorbing capacity, which may have spillover effects to other banks or market participants" & reputational risks to banks and supervisors resulting from high-profile digital fraud incidents (eg enhanced by wide press coverage, public discontent). This could translate to a broader, system- wide loss of trust in the integrity and resilience of banks that could lead to, for example, mass bank deposit withdrawals.*

[5] See: https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Illicit-financial-flows-cyber-enabled-fraud.pdf.coredownload.inline.pdf

[6] See: https://www.police.gov.sg/media-room/news/20230613_regional_anti_scam_conference_2023#:~:text=The Singapore Police Force (SPF,13 to 15 June 2023.

[7] See: https://www.gov.uk/government/news/international-agreement-to-fight-fraud-secured

[8] See: https://www.gov.uk/government/publications/communique-from-the-global-fraud-summit/global-fraud-summit-communique-11-march-2024.

[9] See: https://www.accc.gov.au/system/files/targeting-scams-report-activity-2023.pdf

[10] See: https://futurecarecapital.org.uk/latest/fraud-victims-experience-mental-health-problems/#:~:text=Three in five fraud victims go on to experience mental health problems&text=Three in five (60%),by the government campaign Stop!

[11] See:https://www.fbi.gov/contact-us/field-offices/memphis/news/sextortion-a-growing-threat-targeting-minors

[12] See: https://www.gcffc.org/wp-content/uploads/2024/04/GCFFC_-MS_HT-Proceeds-at-US498B.pdf

[13] See: https://www.usip.org/sites/default/files/2024-05/ssg_transnational-crime-southeast-asia.pdf

[14] See: https://www.theguardian.com/technology/article/2024/may/17/uk-engineering-arup-deepfake-scam-hong-kong-ai-video

[15] See: https://thefinancialcrimenews.com/payment-fraud-scams-against-individuals-businesses-focus-on-uk/

[16] See: https://www.ft.com/content/f85d8bdb-8405-437b-a429-89e737a943fc

[17] See: https://www.interpol.int/en/News-and-Events/News/2024/INTERPOL-Financial-Fraud-assessment-A-global-threat-boosted-by-technology

[18] See: https://www.interpol.int/News-and-Events/News/2023/Americas-257-suspected-migrant-smugglers-and-human-traffickers-arrested

[19] See: https://www.demandsage.com/how-many-emails-are-sent-per-day/#:~:text=How%20Many%20E-mails%20Are,to%20392.5%20billion%20by%202026.

[20] See: https://www.accc.gov.au/system/files/Targeting scams 2022.pdf

[21] See: https://datareportal.com/global-digital-overview#:~:text=There%2520are%25205.35%2520billion%2520internet,higher%2520in%2520many%2520developing%2520economies.

[22] See: https://www.coindesk.com/markets/2021/10/19/australia-has-third-highest-rate-of-crypto-adoption-in-the-world-finder-survey/#:~:text=Almost 18% of the country's population owns crypto.&text=Finder's survey found Australia has,region of China (15.8%).

[23] See: https://www.scamwatch.gov.au

[24] See: https://globalinitiative.net/region/global/

[25] See: https://www.accc.gov.au/system/files/National-Anti-Scam-Centre-in-Action_quarterly-update-October-to-December-2023_0.pdf

[26] See: https://www.accc.gov.au/system/files/National-Anti-Scam-Centre-in-Action_quarterly-update-October-to-December-2023_0.pdf

[27] See: https://www.accc.gov.au/system/files/Targeting scams 2022.pdf

[28] See: https://www.gcffc.org/wp-content/uploads/2020/08/FFIS-Report-Five-Years-of-Growth-of-Public-Private-Partnerships-to-Fight-Financial-Crime-18-Aug-2020.pdf

[29] See: https://www.accc.gov.au/national-anti-scam-centre

[30] See: https://www.scamwatch.gov.au

[31] See: https://www.scamwatch.gov.au/research-and-resources/scams-awareness-week-2023

[32] See: https://download.asic.gov.au/media/mbhoz0pc/rep761-published-20-april-2023.pdf

[33] See: https://www.ausbanking.org.au/new-scam-safe-accord/

[34] See: https://treasury.gov.au/consultation/c2023-464732

[35] See: https://www.afcx.com.au

[36] See: https://treasury.gov.au/consultation/c2023-464732

[37] See: https://www.gov.uk/government/news/international-agreement-to-fight-fraud-secured

[38] See: https://download.asic.gov.au/media/mbhoz0pc/rep761-published-20-april-2023.pdf

[39] See: https://www.afr.com/politics/scams-out-of-control-but-no-move-to-force-banks-to-bail-out-victims-20221104-p5bvoi

[40] See: https://www.police.gov.hk/offbeat/1250/eng/

[41] See: https://www.wenweipo.com/a/202308/21/AP64e2aface4b0fb87b5431db6.html

[42] See: https://hongkongfp.com/2024/01/30/data-breach-notifications-rose-by-nearly-50-in-2023-hong-kong-privacy-watchdog-finds/

[43] See: https://hongkongfp.com/2023/09/13/hong-kong-tech-park-says-data-exposed-by-malicious-hack/

[44] See: https://hongkongfp.com/2023/09/22/hong-kong-consumer-council-falls-victim-to-ransom-hackers-warns-of-suspected-data-breach/

[45] See: https://www.fstb.gov.hk/fsb/aml/en/doc/hk-risk-assessment-report_e.pdf

[46] See: https://www.fstb.gov.hk/fsb/aml/en/doc/Money%2520Laudering%2520Report_2022_EN.pdf

[47] See: https://usa.visa.com/content/dam/VCOM/regional/na/us/Solutions/documents/visa-cryptocurrency-a-and-u-2022-final-white-paper.pdf

[48] See: https://www.fstb.gov.hk/fsb/aml/en/doc/hk-risk-assessment-report_e.pdf

[49] See: https://www.fstb.gov.hk/fsb/aml/en/doc/Money%2520Laudering%2520Report_2022_EN.pdf

[50] See: https://www.hkma.gov.hk/media/eng/doc/key-information/speeches/s20240131e1.pdf

[51] See: https://cyberdefender.hk/statistics/; https://www.police.gov.hk/offbeat/1250/eng/#1

[52] See: https://www.adcc.gov.hk/en-hk/about-us.html

[53] See: https://www.police.gov.hk/offbeat/1247/eng/9020.html

[54] See: https://cyberdefender.hk/

[55] See: https://cyberdefender.hk/en-us/scameter/

[56] See: https://www.hkma.gov.hk/eng/news-and-media/press-releases/2023/04/20230421-7/

[57] See: https://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2023/20231012e1.pdf%2520%252013%2520October%2520-%2520HKMA

[58] See: https://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2023/20231012e1.pdf%2520%252013%2520October%2520-%2520HKMA

[59] See: https://www.hkma.gov.hk/eng/news-and-media/press-releases/2023/06/20230607-5/

[60] See: https://www.hkab.org.hk/en/news/press-release/270

[61] See: https://www.hkma.gov.hk/eng/news-and-media/press-releases/2024/01/20240123-4/

[62] See: https://www.hkma.gov.hk/media/eng/doc/key-information/speeches/s20240131e1.pdf

[63] See: https://www.hkma.gov.hk/eng/news-and-media/press-releases/2017/05/20170526-3/

[64] See: https://www.hkma.gov.hk/eng/news-and-media/press-releases/2023/06/20230620-5/

[65] See: https://www.wenweipo.com/a/202308/21/AP64e2aface4b0fb87b5431db6.html

[66] See: https://www.ofca.gov.hk/en/consumer_focus/guide/hot_topics/ssrs/index.html

[67] See: https://www.ofca.gov.hk/filemanager/ofca/en/content_1684/Registry_Govt.pdf

[68] See: https://www.gov.uk/government/news/international-agreement-to-fight-fraud-secured

[69] See: mhttps://www.police.gov.sg//-/media/Spf/Media-Room/Statistics/Annual-Scams-and-Cybercrime-Brief-2023/Annual-Scams-and-Cybercrime-Brief-2023.ashx

[70] See: https://datareportal.com/global-digital-overview#:~:text=There%2520are%25205.35%2520billion%2520internet,higher%2520in%2520many%2520developing%2520economies.

[71] See: https://www.mha.gov.sg/mediaroom/parliamentary/committee-of-supply-debate-2024-on-advancing-the-fight-against-scams/

[72] See: https://globalinitiative.net/region/global/

[73] See: https://usa.visa.com/content/dam/VCOM/regional/na/us/Solutions/documents/visa-cryptocurrency-a-and-u-2022-final-white-paper.pdf

[74] See: https://www.police.gov.sg/-/media/8F06592D8FBE475C8D2B92EB3BFFE7FC.ashx#:~:text=The number of scam and,92.4% of these 50,376 cases.

[75] See: https://www.mas.gov.sg/regulation/anti-money-laundering/amlcft-industry-partnership-acip

[76] See: https://www.police.gov.sg/media-room/news/20220906_opening_of_anti-scam_command_office

[77] See: https://www.abs.org.sg/industry-guidelines/fraud

[78] See: https://www.police.gov.sg/media-room/news/20220906_opening_of_anti-scam_command_office

[79] See: https://www.police.gov.sg//-/media/Spf/Media-Room/Statistics/Annual-Scams-and-Cybercrime-Brief-2023/Annual-Scams-and-Cybercrime-Brief-2023.ashx

Financial Scams Report

An Assessment of Scams in East Asia - in Australia, Hong Kong & Singapore

Acknowledgements

Written and Produced by the Global Coalition to Fight Financial Crime (GCFFC), the GCFFC APAC Chapter & APAC Chapter Fraud & Scams Working Group. With special thanks to authors and contributors Rachelle Boyle, Julia Chin, Andrew Chow, John Cusack, Cathy Hoi Sze KUET, Robin Lee, Ursula M'Crystal, Cyril Mak, Sathish Ranganathan, Luke Raven & Rayson Tan, as well as Jodie Arthur and Debra Au as APAC Chapter Co Chairs for their full support of this initiative.

Scam Working Group Co Chairs
Andrew Chow & Sathish Ranganathan

Additional thanks for the Country Working Groups:

Australia
Rachelle Boyle (Lead)
Giselle Lindley
Punit Kaushik
Toby Evans

Hong Kong SAR
Cyril Mak (Lead)
Marina Mai
Byron Philips
Stanley Wu
Dick Lai
Jose L. Sandoval
Vince Turcotte
Edgar Ma

Singapore
Rayson Tan (Lead)
Brandon Lobo
Aaron Lee
Beaver Chua
Maxim Afanasyev