IDEAS | PEOPLE | TRUST

Scams Environment Data Analysis

Westpac

December 2024

Table of Contents

Executive Summary

Reader's note: definition of scams

The definition of 'scam' varies across the Australian scam ecosystem and from country to country. This creates inconsistency in scam data reporting, and makes it difficult to compare jurisdictions on a 'like-for-like' basis. Specific definitional complexities are discussed in detail throughout this report.

The Australian and global scam environment continues to evolve due to technological advancements, increasing economic pressures and more sophisticated scamming techniques. While the approaches used by scammers to target both organisations and individuals are consistent across geographic boundaries, the government's policy approaches to scams can differ from country to country. To better understand how well these different approaches are working, we have conducted analysis to quantify and compare scam activities across jurisdictions. We looked at publicly available data to compare reported scam data across Australia and the UK, and where available for the USA and Canada.[1] Australian data has been sourced from the ACCC.

To ensure consistency with other jurisdictions (such as the UK), this report assesses scam losses in Australia in line with what is reported under the UK's Contingent Reimbursement Scheme and other relevant overseas legislation or reporting metrics. This ensures the best like-for-like comparison between countries; however, means losses in Australia are lower than reported elsewhere.[2] More information about scam loss reporting differences across jurisdictions is detailed on page 20 of this report.

Analysis of the available data identified the following key findings:

- In the UK, per capita scam losses are almost double those in Australia.
- Since the introduction of the UK Contingent Reimbursement Model (CRM), there has been year-on-year growth in reported cases. This is almost four times the rate of scams per capita in Australia.
- While Australian scam losses and cases grew from 2020 to 2023, Australia has seen a 40% reduction in losses in 2024 since banks and government have focused on implementing preventative measures. By comparison, scam losses in the UK, USA and Canada have continued to increase in this same time period.
- The data indicates that an increase in UK scam cases and losses since the introduction of the CRM coincides with an increase in the reporting rate, with minimal impact on actual incurred losses.
- There is also a notable difference in the level of scam reporting between Australia and the UK, with the UK model excluding some scam typologies that are reported in Australia, and excluding some payment channels through which scam payments are authorised.

Comparing jurisdictions

Across a variety of comparative analytics, the UK scam environment appeared to differentiate to the Australian environment, whilst strong comparisons could be drawn between Australia and other jurisdictions, such as Canada and USA. These comparisons identified that Australia reported on average the lowest value of loss per report submitted. In the UK, the reported amount lost per capita to scams ($33.48 AUD) is almost double the amount lost by Australians ($17.69 AUD), with Australian's total loss per scam trending down 40% from 2023 to 2024.

Since the introduction of the UK's Contingent Reimbursement Model (CRM) in May 2019, the UK has recorded year-on-year growth in the number of authorised push payment (APP) scams reported (reimbursable under the CRM) and reported almost four times the rate of scams *per capita* than Australia (0.15 reports per capita

[1] There was limited publicly reported scam data for New Zealand, so that country was not included in this analysis.

[2] Under this approach, scam losses in Australia between [2020 – 2023] ($1.495bn) are lower than the ACCC's reported total ($2.7bn).

in the UK and 0.04 reports in Australia). During this period, the UK's number of reported instances of APP scams increased from 122,437 to 232,469, or by 90%. Conversely, in the period 2020 – 2023 in Australia, the number of reported (equivalent) APP scams remained fairly stagnant. In 2023 in the UK, 62% ($556.98 million) of all APP scam losses were reimbursed to the victims, which is an increase on the reported 59% in 2022.

From 2020 to 2023, Australia saw an increase of 61% in the value of funds lost to scams, coupled with an increase of 22% of scam instances reported. Telecommunications remained the primary solicitation method for scams within Australia, however, 47% of losses were attributable to scams initiated online. Investment scams caused the greatest monetary loss in Australia throughout the period, with remote access scams (where the victim is not aware of the crime, refer Appendices 1 and 2) being the most reported on.

In the same period, the UK reported 10,535,777 instances of scams totalling $8.796 billion. As opposed to Australia, online remained the primary solicitation method for scams in the UK, with 45% of losses however being attributable to scams initiated via Telecommunications. The UK further reported that Remote Access scams were both the most reported on and caused greatest monetary loss.

The UK data shows that during the period 2019 – 2023 the number of reported instances of APP scams increased from 122,437 to 232,469, or by 90%. During the same period, losses due to APP scams have fluctuated year-on-year, with an actual increase in total losses identified in the period (1%). This suggests that the implementation of the CRM in the UK appears to have coincided with an increase in the reporting rate of APP scams but has had minimal impact on actual losses incurred by individuals due to APP scams. In addition to this, UK Finance reported that in 2023 62% ($556.98 million) of all APP scams were reimbursed to the victims, which is an increase on the reported 59% in 2022.

In the same period, UK reported losses amounting to $8.796 billion with 10,535,777 reported instances (0.15 reported instances per capita). The data suggests that both Canada ($13,098.48 in 2023) and USA ($5,370.25 in 2023) on average are losing a greater value of money per report when compared to Australia ($939.66 in 2023). The increasing total loss per report in both Canada and USA over this period contrasts with Australia where, in the same period, Australians' total loss per report has trended downward, with a 40% drop in the year from 2023 to 2024, coinciding with a significant uplift in scam prevention measures and efforts from banks, telcos and government.

Scope

BDO was engaged to conduct a comparative analysis over publicly available scam data across Australia and the United Kingdom as well as any additional similar jurisdictions. The intention of the analysis is to quantify and compare the scam environment and respective customer losses across jurisdictions, for Westpac to consider the efficacy of respective scam intervention policies. The scope of the engagement includes:

- Collection of scam loss data in Australia and United Kingdom (UK) over a five-year period from publicly available information.
- Ensure the collected data categorises scams in a like-for-like comparison across jurisdictions
- Provide additional high-level data comparisons for comparable jurisdictions
- Provide consideration of the downstream impacts of different regulatory approaches across jurisdictions
- Comparative analysis over reported APP scam data (UK) and banking data reported to ASIC (Australia)

This high-level report sets out our significant observations based on publicly available scams data in Australia, the United Kingdom (UK), Canada and the United States (US).

Approach

In researching and collecting jurisdictional data, it was identified that only Australia and Canada provided detailed raw data of reported scam or fraud instances. Both the UK and US provided only reports/dashboards of scam findings. We had to accept reliance over the reporting agency's ability to report findings over the scam and fraud data (limitations are further stipulated at page 22). Additionally, meaningful Australian scam data was only able to be extracted for the year commencing 2020, therefore the analysis period has been determined as January 2020 – June 2024.

Following collection of the data, to ensure comparison of like-for-like scam data (insofar as possible), scam types in each dataset had to be categorised in the following BDO formulated broad categories:

- Romance - the criminal adopts a fake online identity to gain the victim's affection or trust.
- Investment – the scammer attempts to 'trick' an individual into investing money.
- Remote Access – a criminal acquires remote access to a victim's bank account or credit card.
- Unexpected Winnings – the victim is tricked into providing financial details to claim a prize.
- Buying/Selling – fake online sellers of services and goods that do not exist.
- Job and Payment Scams – victims are asked to provide financial details to obtain a job
- Impersonation/Threats – criminals impersonate law enforcement to obtain victim details.[3]
- Identity Theft – a victim's credit card or financial details are stolen via online hack.
- Other – miscellaneous reported scam types.

A detailed description of the specific scam types which make-up the individual categories is provided in Appendix 2.

Scam versus fraud – definitional complexities

The definition of 'scam' varies between jurisdictions, which in turn affects the nature of data reporting. Broadly, when the victim are themselves not involved in initiating or facilitating the transaction, the instance may be deemed a 'fraud' in the UK, and thereby not captured or reported. In contrast, the Australian data includes this type of transaction in the reported 'scam' data. In the UK, the narrower definition of 'scam' is transactions whereby the victim involved *initiates* or *facilitates* the transaction, including under a false belief as to where and/or to whom the funds are going. This is referred to as Authorised Push Payments (APP).

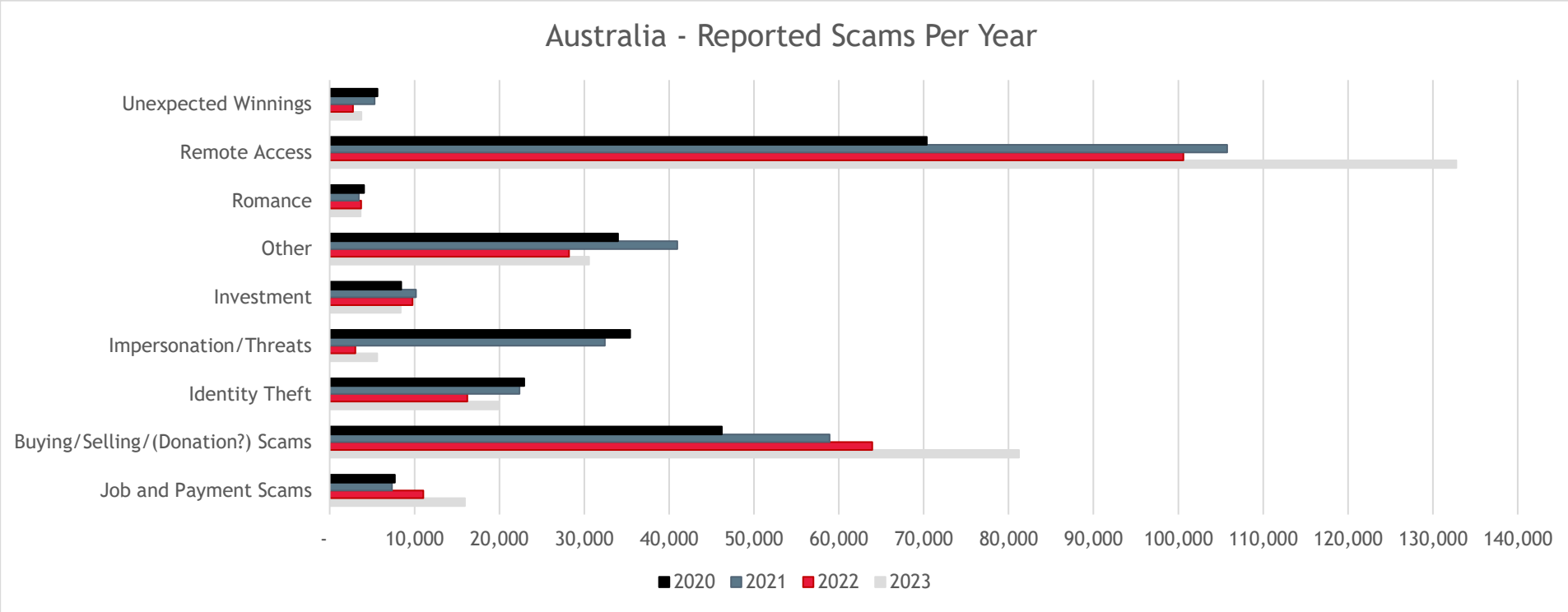
For this review, we conducted an additional detailed categorisation of APP scam data based on the UK's categorisation of these scam typologies. To the extent possible, a like-for-like comparison of APP scam categorisation versus the Australian scam types was conducted (Appendix 4). However, due to inherent limitations in the ability of like-for-like comparison between UK APP scam types and Australian scam types (e.g. UK publicly available data does not disaggregate its individual scam types), a conservative approach in determining the Australian scam types which would be classified as an APP scam has been adopted. N.B. The Australian reported 'scam' data therefore includes typologies that would be considered *fraud*, and therefore not a reportable scam, under the UK model.

This complexity in analytical comparisons underscores the importance of having an agreed and consistent scam reporting taxonomy for Australia.

[3] For ease of analysis, impersonation and threat scams have been combined, as the category 'threat' exists in the Australian data but not in UK data, whereas the 'impersonation' category does not exist in the Australian data but is present in the UK data.

Reported scams per year: Australia & the UK

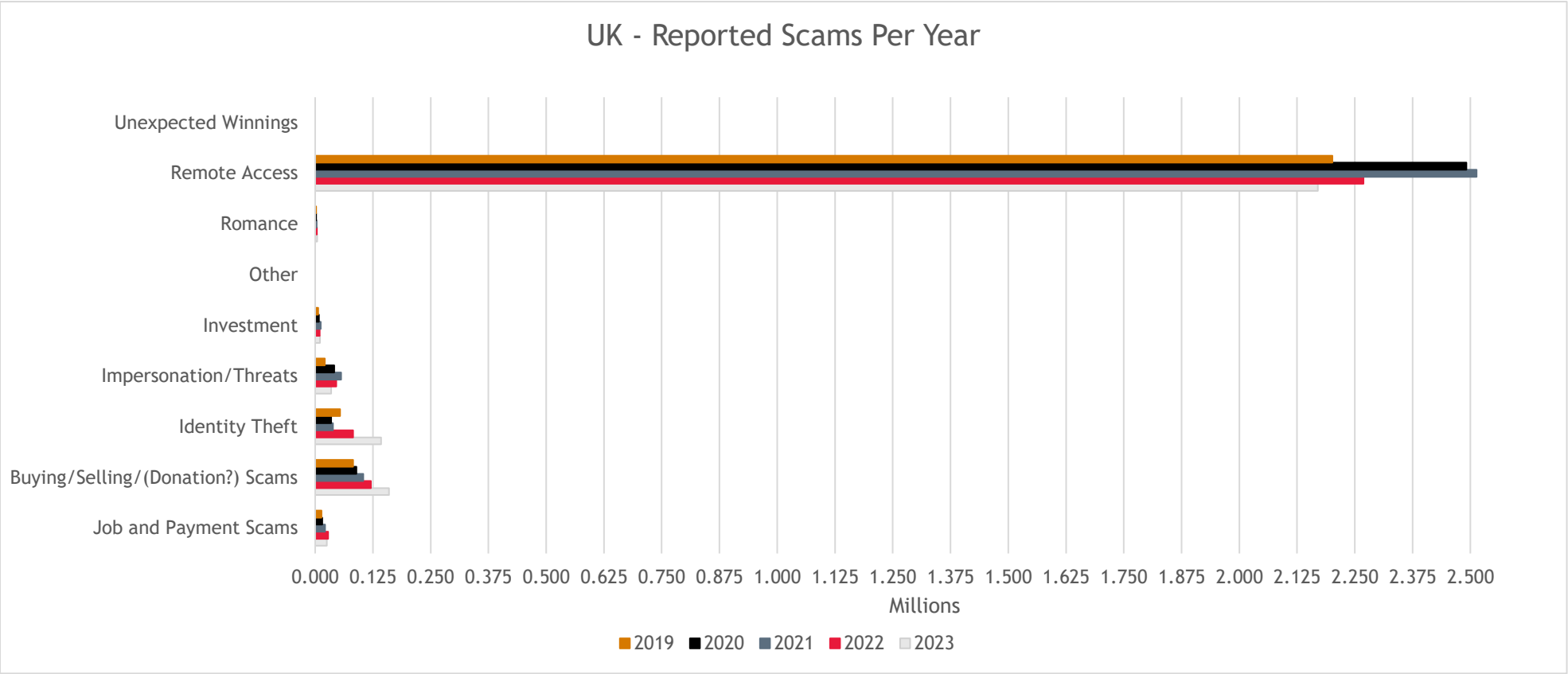
In the period January 2020 – December 2023, Australia reported losses of $1,495 billion directly incurred due to scams and fraudulent activities, with reported instances totalling 1,062,301 (0.04 reported instances per capita[4]). In the same period, UK reported losses amounting to $8.796 billion with 10,535,777 reported instances (0.15 reported instances per capita[5]). This suggests that the UK has almost four times the scam rate per capita than Australia. Of the scams and fraudulent activities reported to Australian entities, it can be identified that remote access scams were the most reported, with all remaining categories appearing to be well reported across each year. Similar to Australia, the greatest reported scam category in the UK was remote access scams, with reporting levels remaining fairly consistent. However, the remaining scam categories in the UK are less reported in comparison to remote access scams[6].



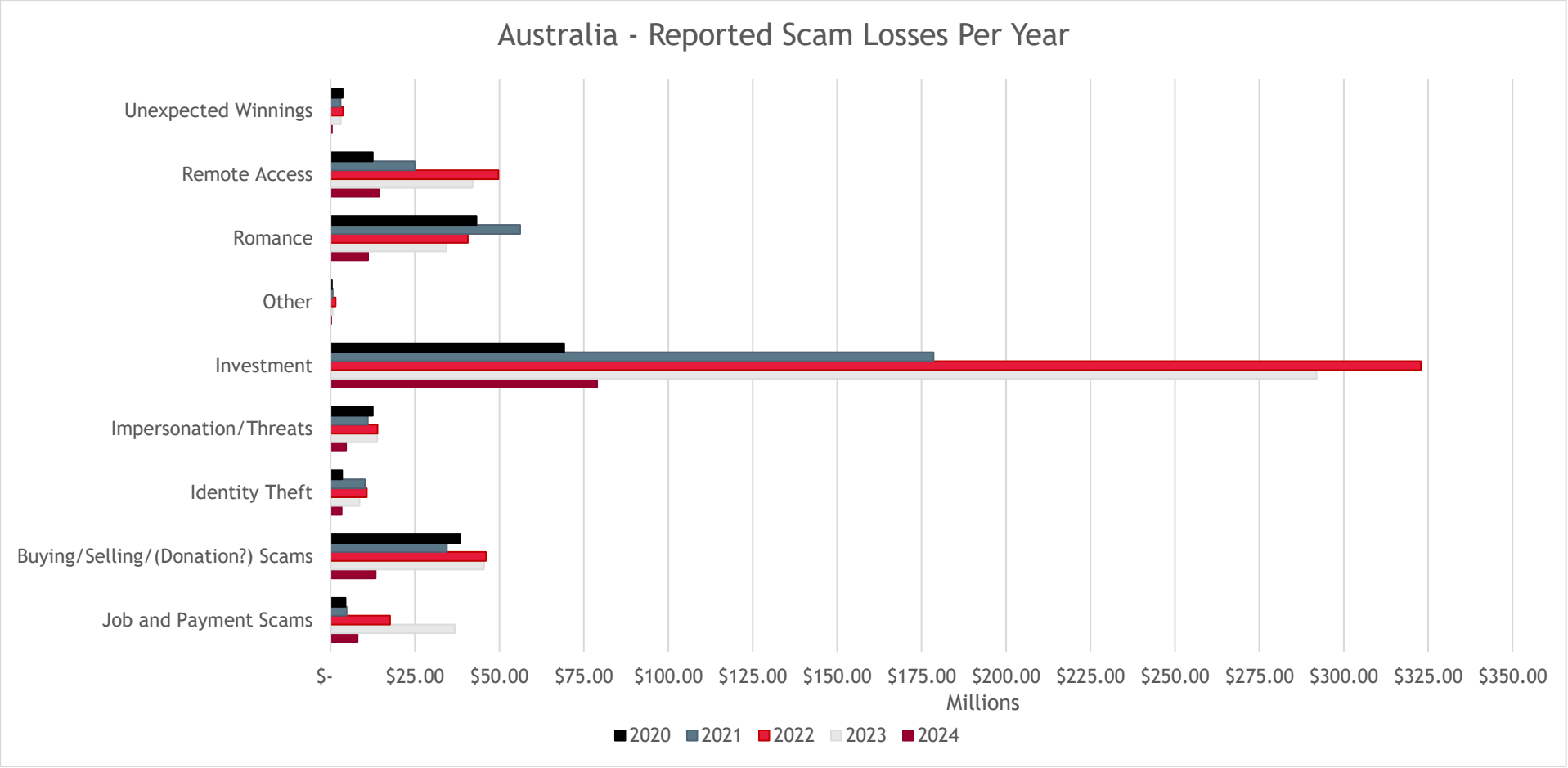
[4] The 2023 Australian population data has been used to determine per capita values

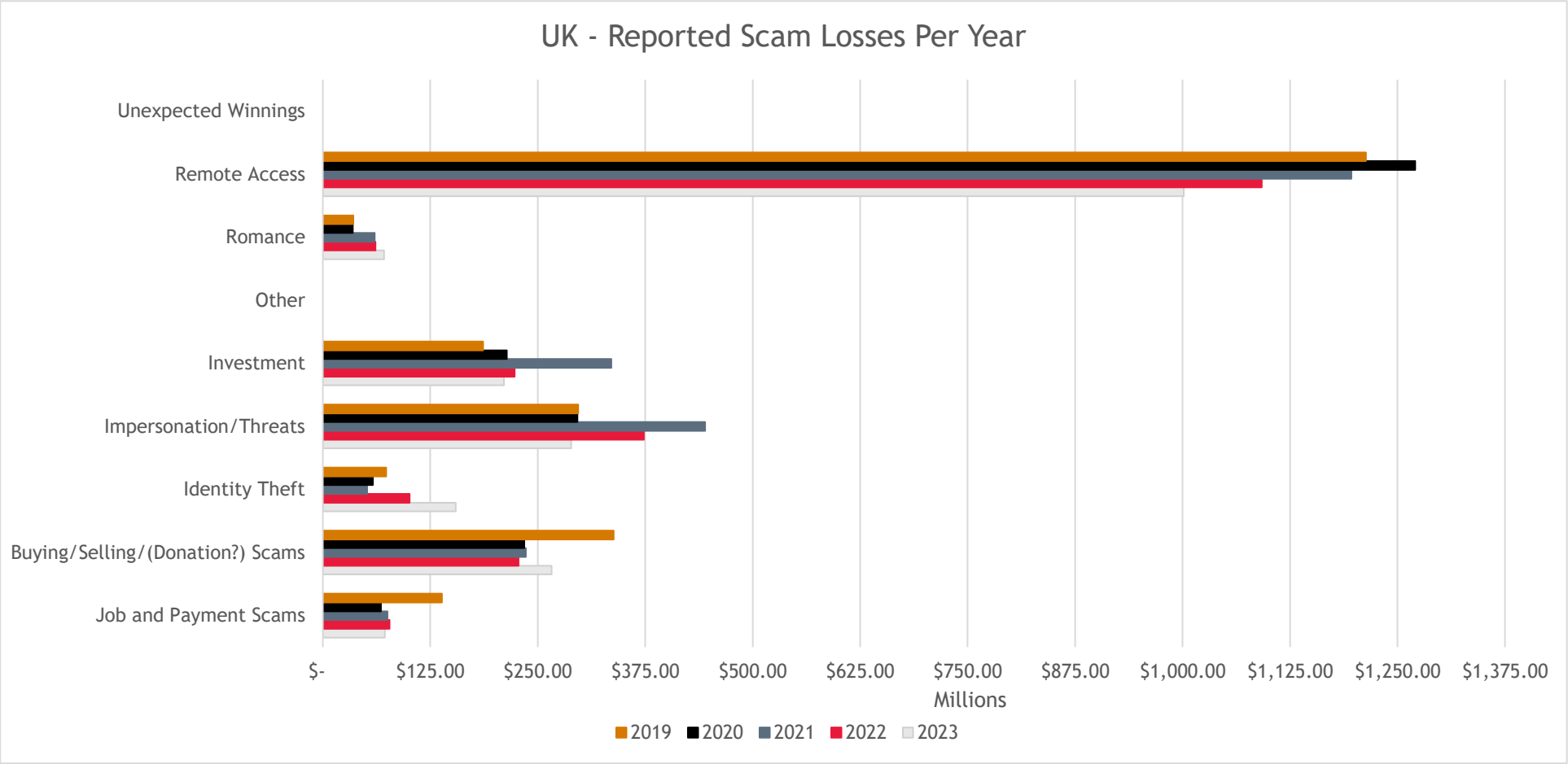
[5] The 2023 United Kingdom population data has been used to determine per capita values

[6] In the graphical analysis the 2019 UK data has been removed as there is no comparable date range in the Australian data. Additionally, the 2024 to date Australian data as there is no comparable date range in the UK data.

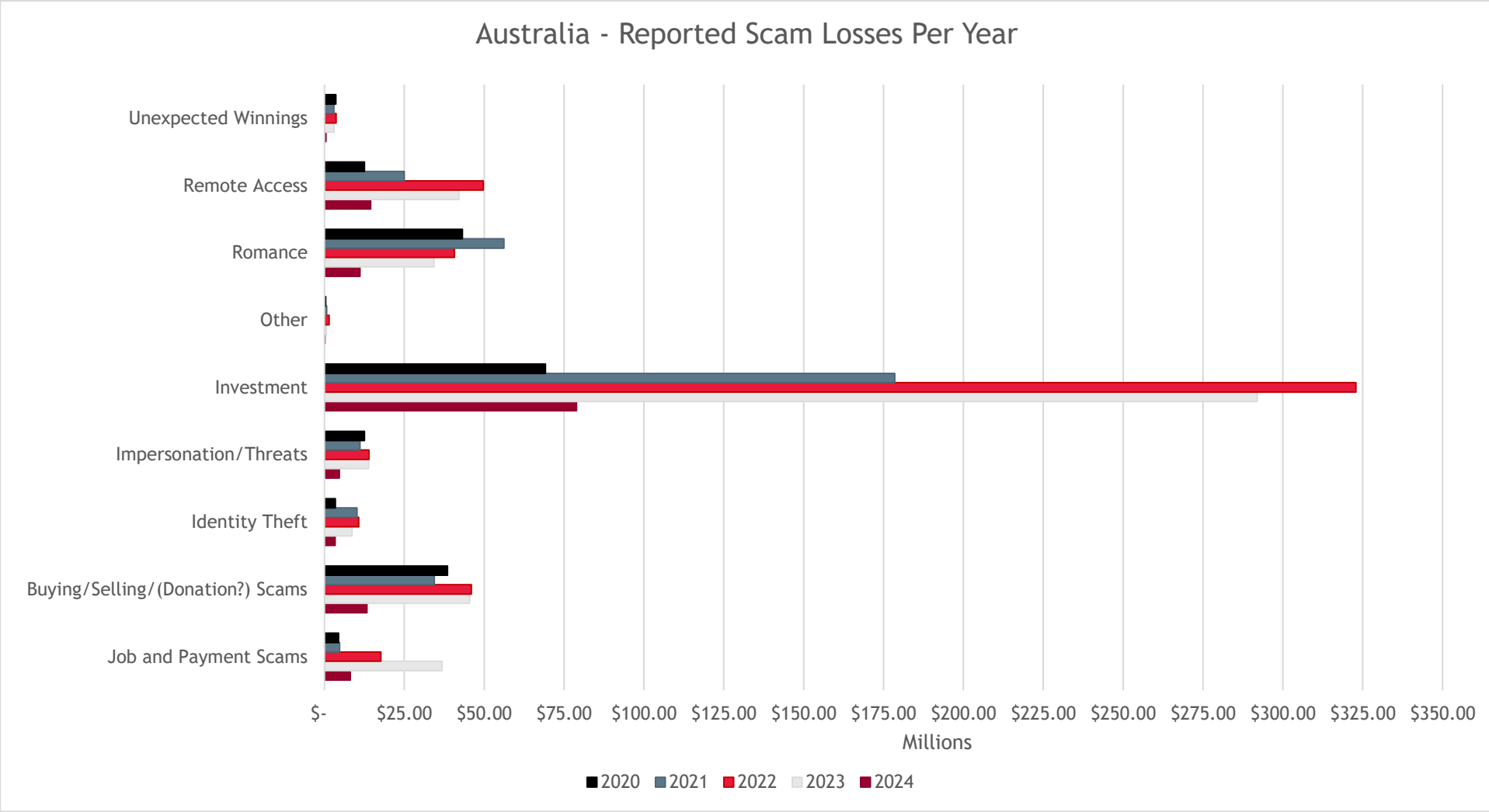

UK - Reported Scams Per Year
Unexpected Winnings
Remote Access
Romance
Other
Investment
Impersonation/Threats
Identity Theft
Buying/Selling/(Donation?) Scams
Job and Payment Scams
0.000 0.125 0.250 0.375 0.500 0.625 0.750 0.875 1.000 1.125 1.250 1.375 1.500 1.625 1.750 1.875 2.000 2.125 2.250 2.375 2.500
Millions
2019 2020 2021 2022 2023

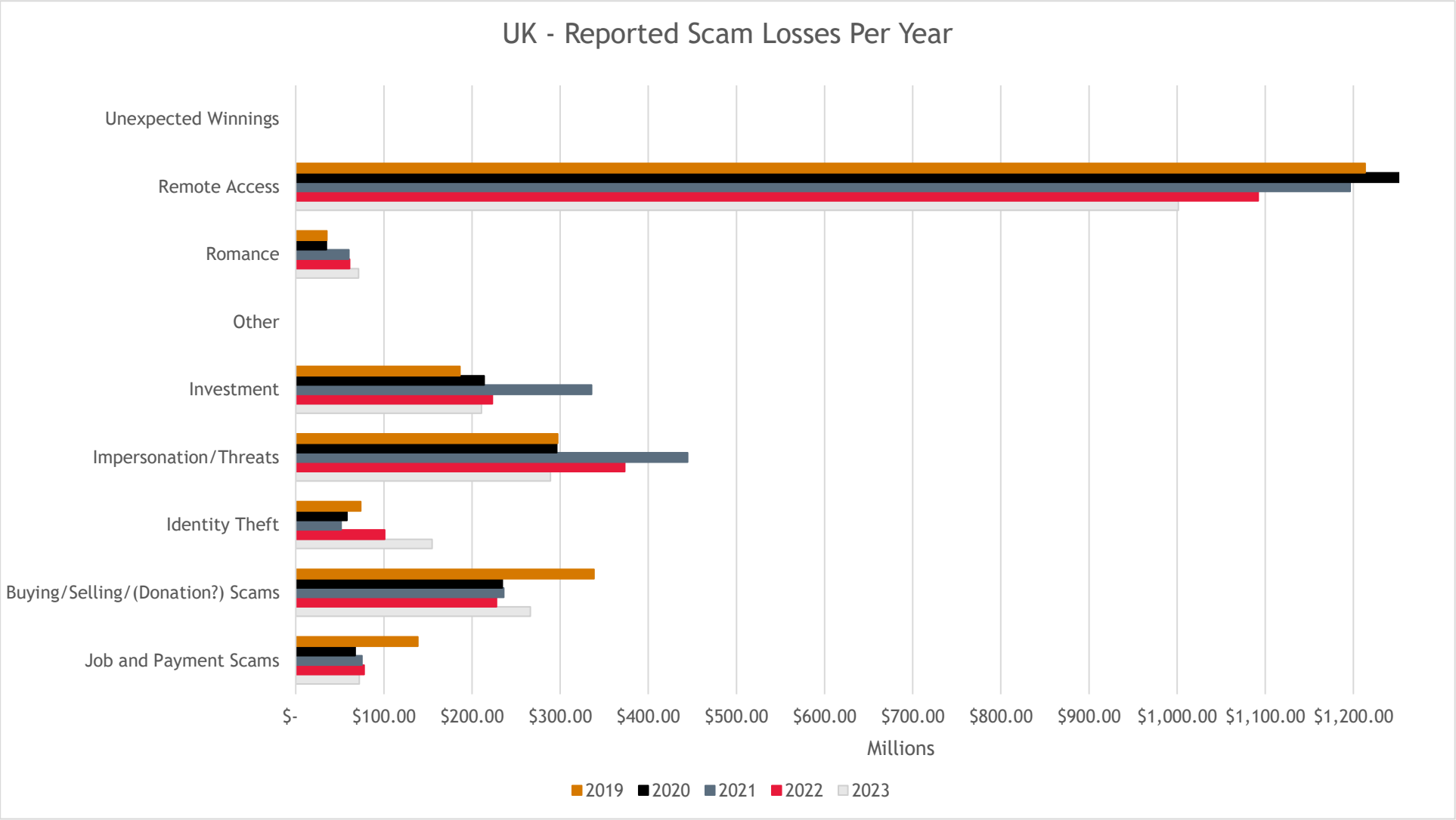
When looking at the amounts lost per scam category, the data demonstrates that investment scams caused the greatest monetary loss in Australia. Interestingly, investment scams are reported at a lower level, which could be impacted by the adopted definition of 'investment' scam. It could also be that Australians are lacking in their ability to identify investment scams, and in turn are losing greater amounts due to this. The UK appears to report differing results. As opposed to Australia, the UK appears to be incurring losses at a greater rate than scams are being reported to reporting agencies across a majority of scam categories. This could be for a variety of reasons; for example, a reduced understanding of scam threats or a more relaxed approach to scams due to the implementation of the Contingent Reimbursement Model.



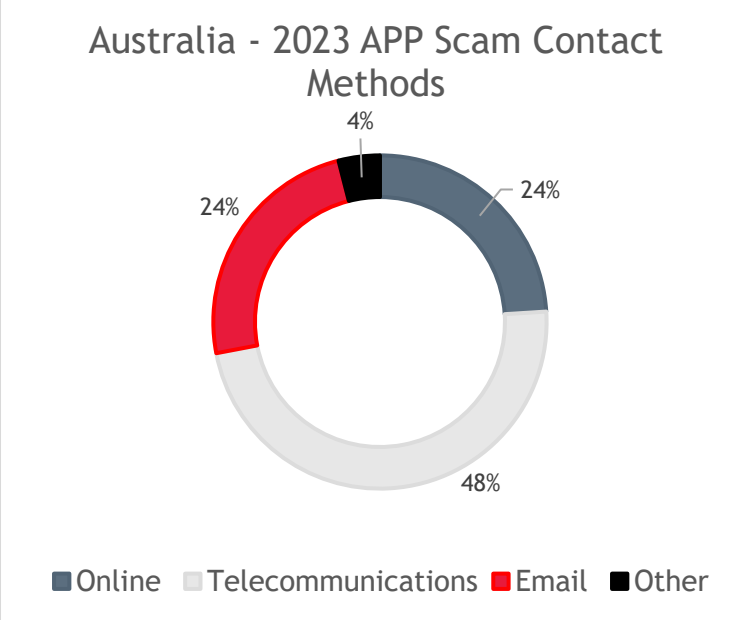

UK - Reported Scam Losses Per Year
Unexpected Winnings
Remote Access
Romance
Other
Investment
Impersonation/Threats
Identity Theft
Buying/Selling/(Donation?) Scams
Job and Payment Scams
$-
$125.00
$250.00
$375.00
$500.00
$625.00
$750.00
$875.00
$1,000.00
$1,125.00
$1,250.00
$1,375.00
Millions
2019
2020
2021
2022
2023

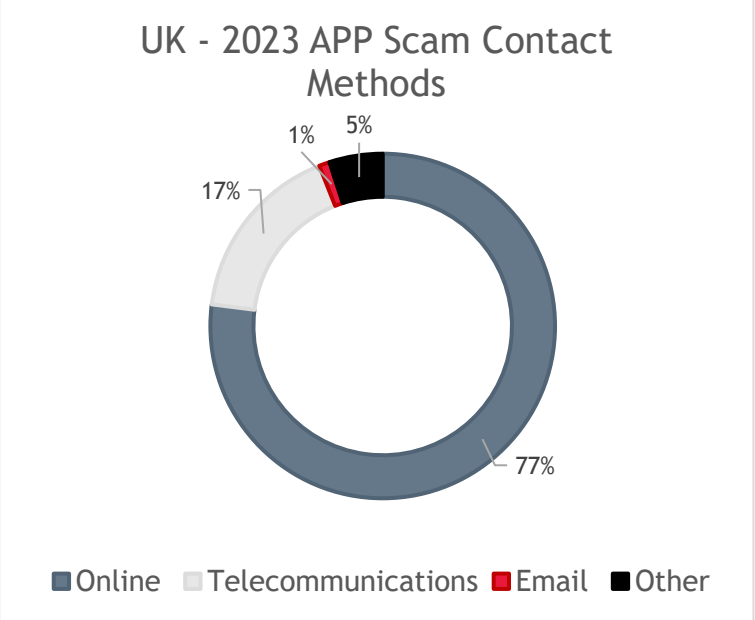
Where a narrowed definition of scams is implemented, whereby, a scam is defined as a transaction authorised or facilitated by an individual including under a false belief as to where and/or to whom the funds are going, the “Remote Access” categorisation is removed. The removal of this categorisation causes minimal change to the Australian data; however, a noticeable shift is recognised in the UK data. The UK data shows that several categorisations record consistently high scam losses in comparison to the Australian data.



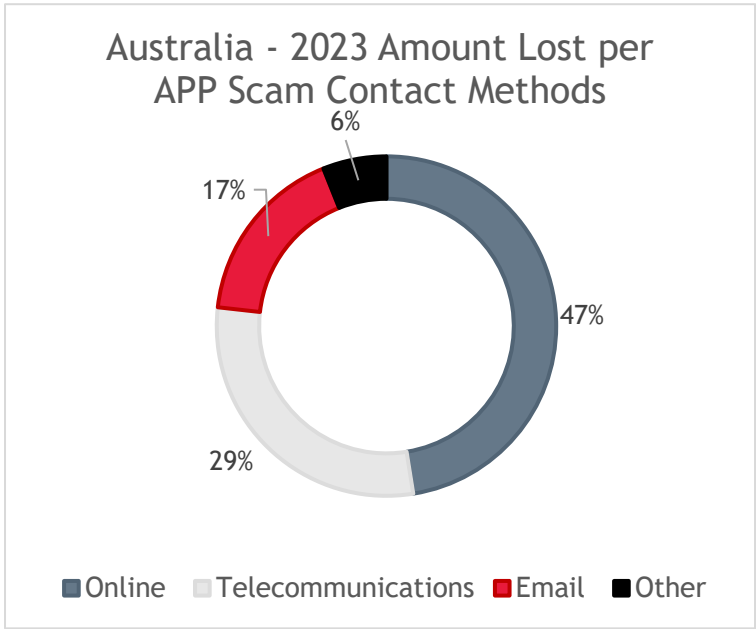

UK - Reported Scam Losses Per Year
Unexpected Winnings
Remote Access
Romance
Other
Investment
Impersonation/Threats
Identity Theft
Buying/Selling/(Donation?) Scams
Job and Payment Scams
$-
$100.00
$200.00
$300.00
$400.00
$500.00
$600.00
$700.00
$800.00
$900.00
$1,000.00
$1,100.00
$1,200.00
Millions
2019
2020
2021
2022
2023

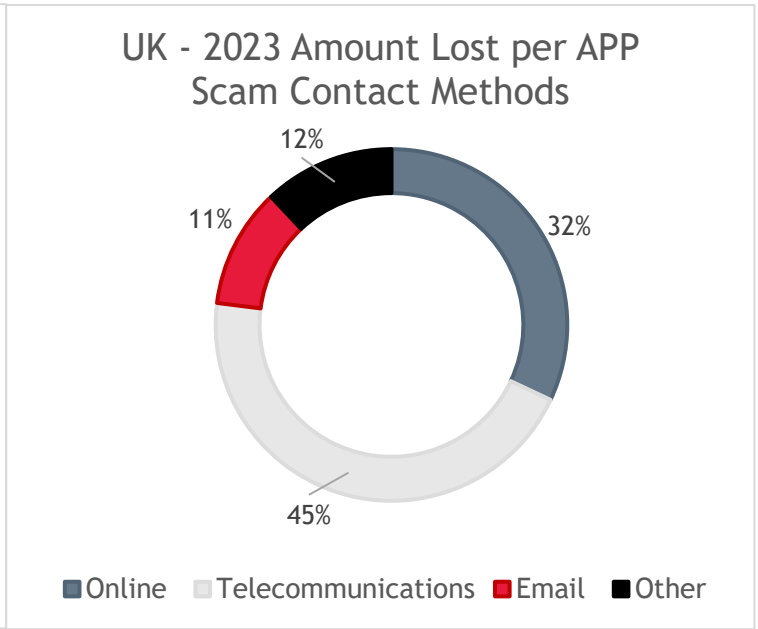
As of 28 May 2019, the UK introduced the CRM, where individuals may be eligible for reimbursement if scammed. A stipulation of the CRM is that reimbursements are only provided on APP scam losses (see Appendix 4 for APP categorisation). The UK provides data on the contact methods which scammers utilise for APP scams. The data suggests that a majority (77%) of APP scams are initiated through online methods (websites, social media etc.). In comparison, the most frequent contact method for Australia is telecommunications (48%), with online methods accounting for around a quarter of responses. However, when analysis is conducted over the amounts lost from each contact method a different outcome is produced.





In the UK, of the funds lost through APP scams, 45% appear to have been solicited through telecommunication methods, this suggests that the UK may be struggling to identify scams solicited via telecommunication due to the significant disparity between instances reported and amount lost. A similar occurrence was identified in the Australian data, whereby scams solicited through online methods accounted for 47% of amounts lost in APP scams.

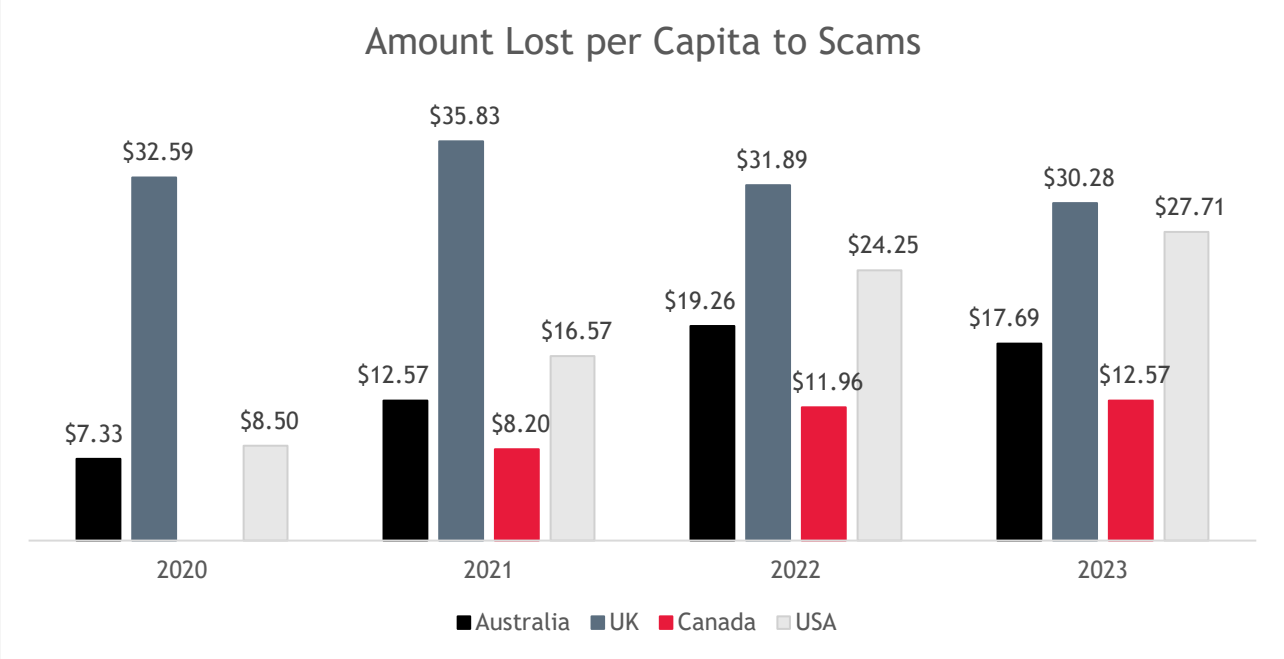




Losses per capita: all countries

Analysis of amounts lost per capita provides a more granular view of how Australian and UK residents are being financially impacted by scams. On average, a UK individual lost $30.28 in 2023 scams. In Australia, scam victims reportedly lost on average $17.69 in 2023. Although the UK data appears to be on a downward trend, the reported amounts lost per capita are roughly twice that demonstrated in the Australian data. This is despite the fact that the amount lost per capita in Australia has increased roughly 2.5 times between 2020 and 2023. So, while the number of reported scams in Australia is increasing, actual losses for each Australian are diminishing while UK resident losses remain stubbornly high with each UK resident losing almost twice as much as Australians per scam.

We looked at the USA and Canada for any observable trends in their scam losses. Between 2020 and 2023, the USA has recorded steady increases in the amount lost per capita year-on-year, with average loss per US resident in 2023 being $27.71 (AUD). Likewise, the amount Canadians have been losing has risen consistently between 2021 and 2023, although of the four countries examined, they continue to report the lowest overall losses per resident[7].



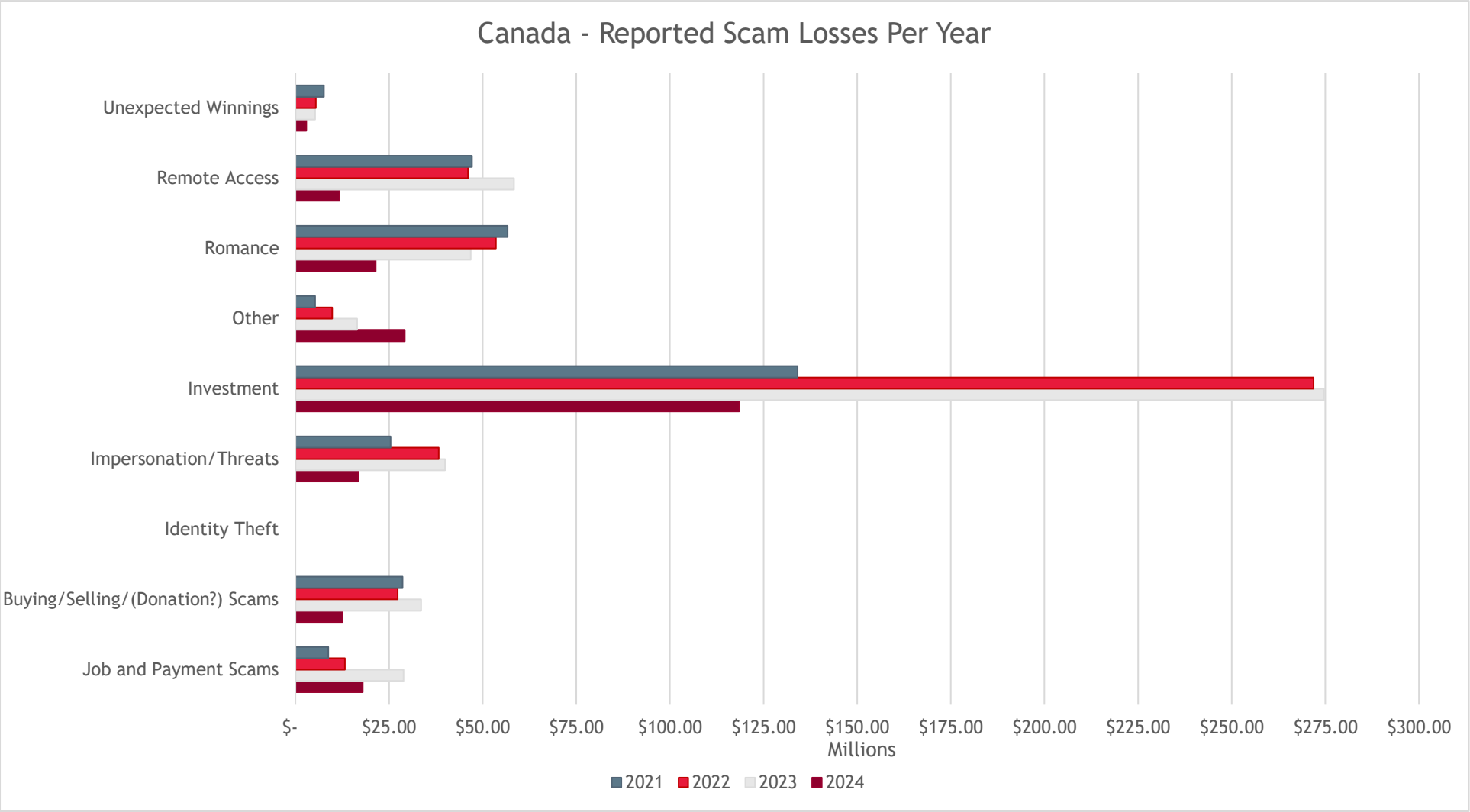
Reported scams per year: USA & Canada

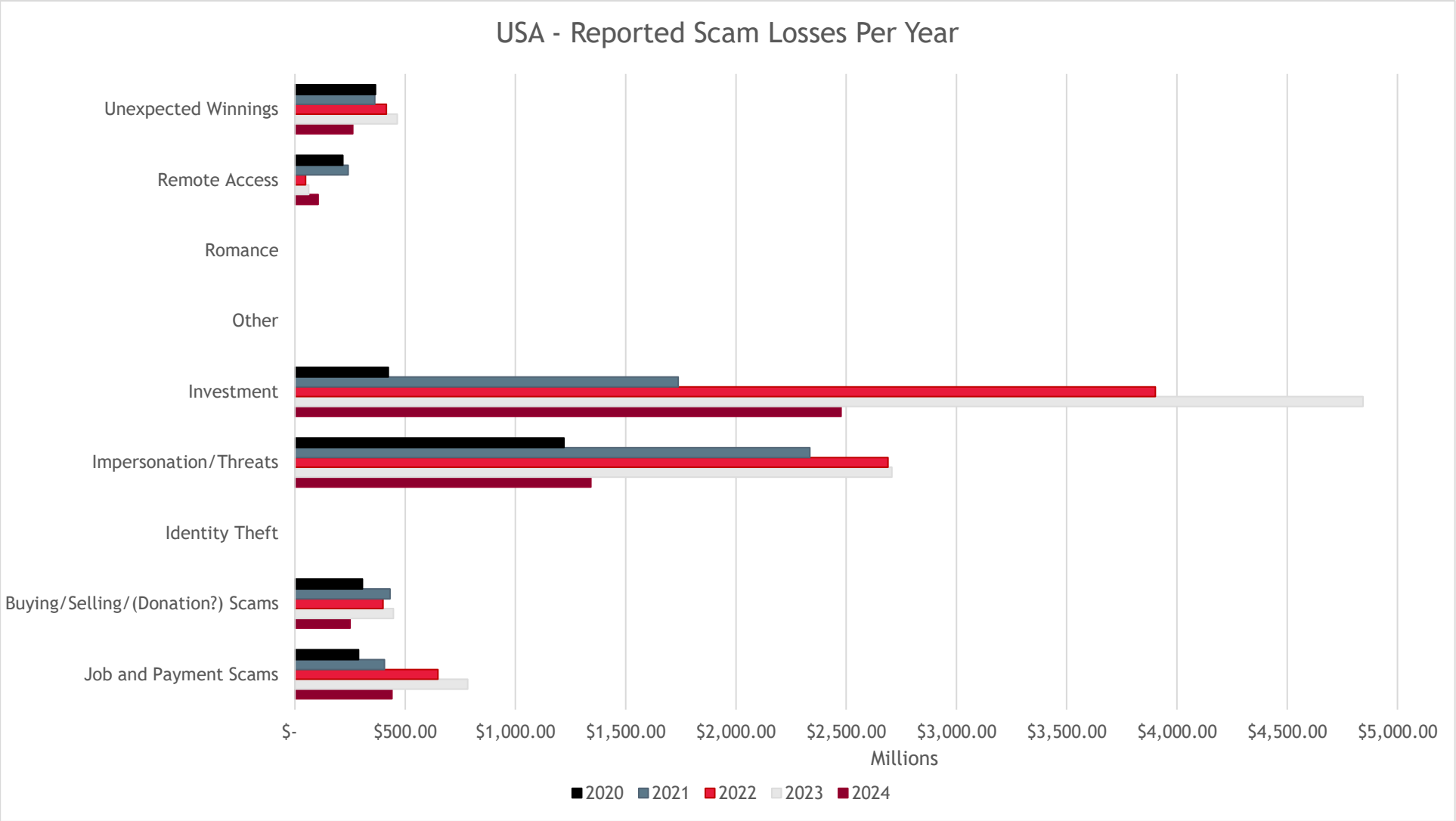
Total losses

In the period January 2021 – December 2023, Canada reported total losses of $1.283 billion directly incurred due to scams and fraudulent activities, with reported instances totalling 198,718. In the period January 2020 – December 2023, USA reported losses amounting to $25.745 billion with 8,097,755 reported instances.

[7] Publicly available data from 2020 for the Canadian jurisdiction could not be identified.

In terms of amounts lost per scam category, both Canada and USA appear to follow a similar trend to the Australian data. Investment scams is the category with the greatest value of losses in Canada and the USA, across all periods data is available. However, the USA ($2,707.10 million) loses a noticeable value of funds to Impersonation/Threats scams, whereas in Australia ($13.86 million) total losses to this scam type are much less significant.




USA - Reported Scam Losses Per Year
Unexpected Winnings
Remote Access
Romance
Other
Investment
Impersonation/Threats
Identity Theft
Buying/Selling/(Donation?) Scams
Job and Payment Scams
$-
$500.00
$1,000.00
$1,500.00
$2,000.00
$2,500.00
$3,000.00
$3,500.00
$4,000.00
$4,500.00
$5,000.00
Millions
2020
2021
2022
2023
2024

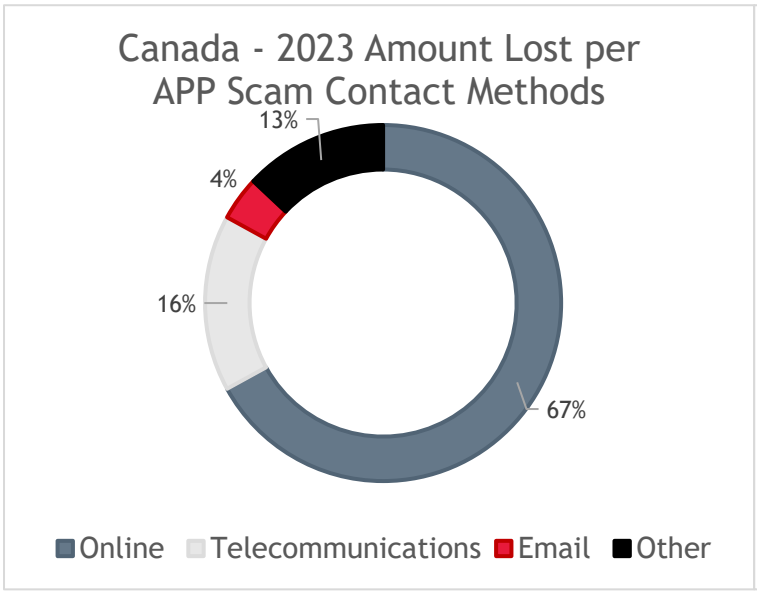
Average losses

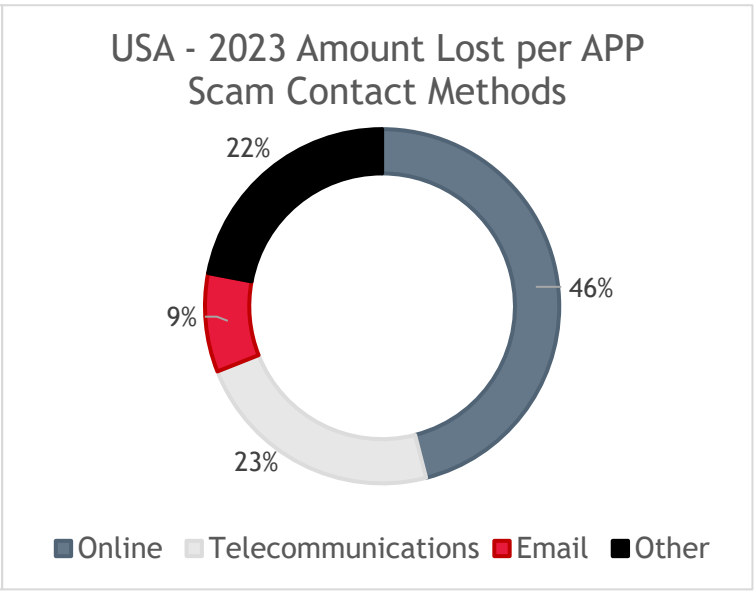
The data suggests that both Canada ($13,098.69 in 2023) and USA ($5,370.25 in 2023) on average are losing a greater value of money per report when compared to Australia ($939.66 in 2023). The increasing total loss per report in both Canada and USA over this period contrasts with Australia where, in the same period, Australians' total loss per report has trended downward, with a 40% drop in the year from 2023 to 2024.

	Australia	Canada	USA
2020	$800.17	$-	$1,654.08
2021	$1,129.44	$4,088.12	$2,354.54
2022	$2,117.86	$6,585.25	$4,065.57
2023	$1,579.96	$9,818.21	$4,523.44
2024	$939.66	$13,098.69	$5,370.25

Scam contact methods

The Canadian and USA data again follows a similar trend to Australia, where the greatest value of funds lost were solicited through an Online method. The main contact method differentiation between Australia and the North American jurisdictions is where Australians (17%) lose a larger total proportion of total scam losses to email as compared with Canada (4%) and USA (9%).



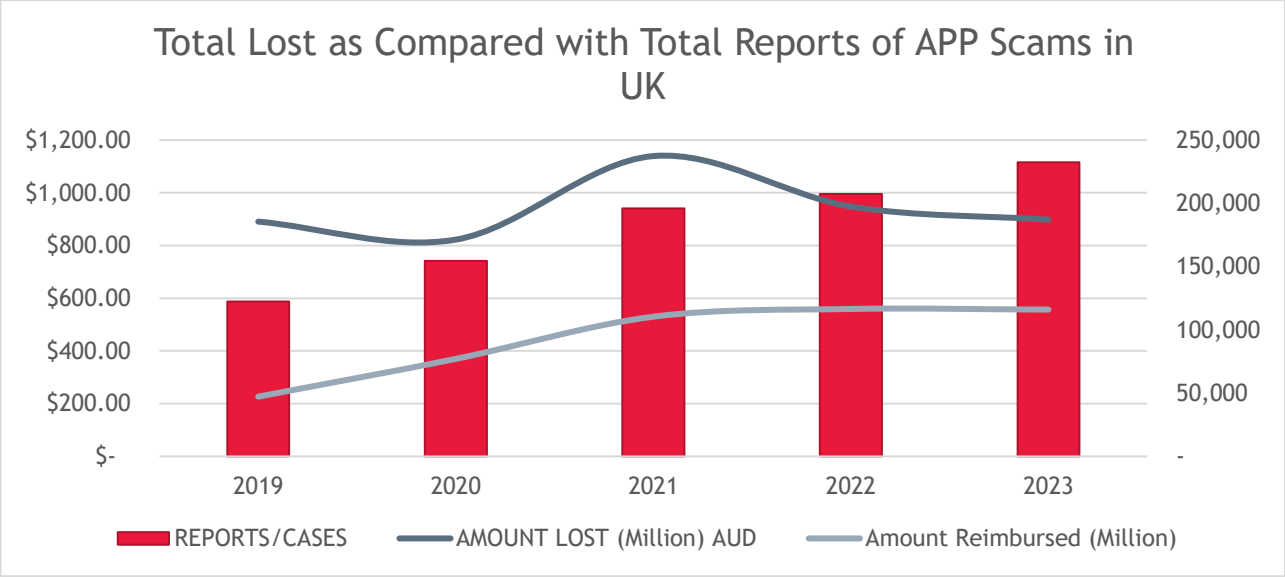


The UK's Contingent Reimbursement Model

On 28 May 2019, the UK government implemented the CRM which aimed to reduce occurrence and impact of APP scams for individuals[8]. At a high level, the CRM seeks to have financial institutions provide reimbursement to individuals who have fallen victim to an APP scam but acted appropriately (i.e. the individual was 'tricked' into authorising payment to an account believing it to belongs to a legitimate payee).

The CRM was previously a voluntary model until it became mandatory on 7 October 2024. However, the major UK banks[9] had been utilising the CRM model prior to 7 October 2024, which according to the UK Lending Solutions Board, accounts for 90% of APP scam data. BDO understands that UK banking institutions report the occurrences of APP scams where they meet the criteria set out by the CRM, whereas Australian reporting entities include a broader range of transaction types that are reported as scams to relevant regulators. As such, there are inherent limitations on the analysis due to an unknown quantity of potentially unreported scams which do not meet the UK's CRM criteria. The difference between the Australian and UK reported scam data are explained in additional detail in the "*Comparing scam reporting*" section on page 21.

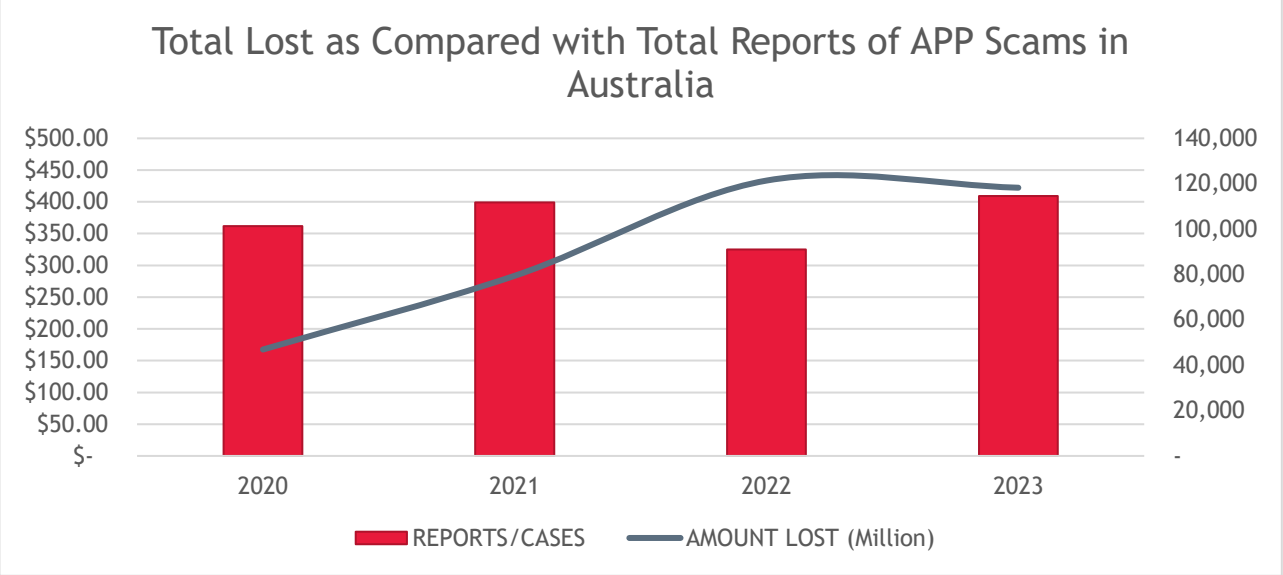
The UK data shows that during the period 2019 – 2023 the number of reported instances of APP scams increased from 122,437 to 232,469, or by 90%. The increase in reports may be in line with expectations as it could be reasonable to anticipate that individuals would be more willing report scams where there is a possibility of reimbursement of funds lost. Over the same period, losses due to APP scams have fluctuated year-on-year, with an actual increase in total losses identified in the period of 1%. The implementation of the CRM in the UK appears to have coincided with an increase in the reporting rate of APP scams but has had minimal impact on actual losses incurred by individuals. In addition to this, UK Finance reported that in 2023, 62% ($556.98 million) of all APP reportable losses were reimbursed to the victims, which is an increase on the reported 59% in 2022.



[8] *Contingent Reimbursement Model Code for Authorised Push Payment Scams,* section OP1.

[9] UK major banks currently utilising CRM model: Barclays Bank UK plc, The Co-Operative Bank Plc, HSBC UK, Lloyds Banking Group, Metro Bank, Nationwide Building Society, NatWest Bank plc, Santander UK, Starling Bank, Virgin Money UK, TSB Bank plc, Monzo Bank Limited, Danske Bank A/S and Allied Irish Banks plc.

For comparative purposes, in a similar period (2020-2023[10]), Australia reported relatively stagnant reporting levels of APP scams, contrary to the year-on-year increases experienced in the UK. Australia did report steady increases in amounts lost to APP scams between 2020 to 2022, however, these appear to have plateaued in 2023. Furthermore, based on the six-month 2024 Australian data available to date, it is possible that there will be a continuation of the downward trend in total amount lost to APP scams.



[10] Publicly available data from 2019 for the Australian jurisdiction could not be identified.

ASIC Reported Scam Data

On 20 August 2024, ASIC released a report on scam data reported by 15 Australian authorised deposit-taking institutions (outside the 4 major Australian banks). The report also included previously reported data from Australia's four major banks. An initial review indicated that ASIC's reported data differs from the ACCC Scamwatch data analysed in the prior sections of this report. It is noted that Scamwatch data incorporates a much broader group of reported scams that includes reports from individuals and businesses. The broader approach to reporting that is included in the Scamwatch reports may include data on transactions that would not be included if the narrower APP focused definition of scam activity[11] is adopted.

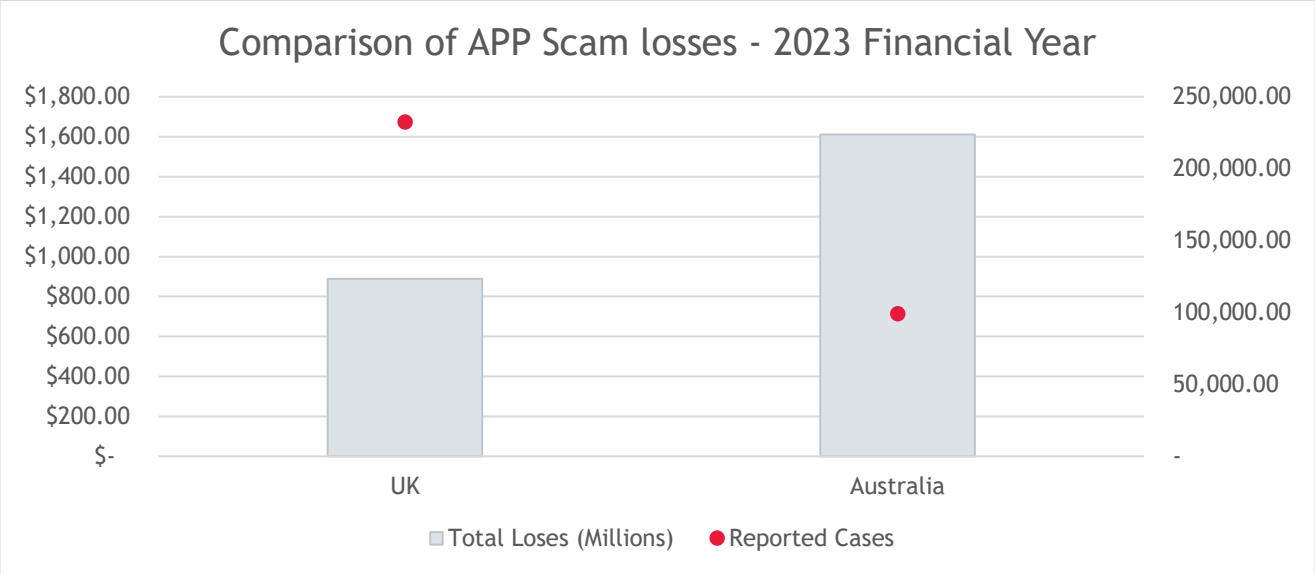
The ASIC report adopts the narrower definition of scams for reporting purposes where scams are considered "situations where customers authorised the transaction by either making the transaction or aiding the scammer to make the transaction, including by providing multi-factor authentication passwords". This definition does appear more comparable to the APP scam data approach as reported by the UK.

Of the findings recorded in the ASIC report, only one full financial year of Australian data was available for comparative purposes across jurisdictions. The ASIC report found that in the 2023 financial year, 99,096 scam cases (those who experienced financial loss) amounting to a total loss of $1.612 billion were recorded across 19 Australian banks (including the 4 major Australian banks).

Comparatively, in the same period, the UK reported 232,429 APP scam cases totalling $0.888 billion (AUD). BDO understands the UK APP scam data excludes transactions whereby:

- A business incurred financial losses due to APP scams and
- The financial loss incurred was sent to a non-GBP-denominated account (account not domiciled within the UK)

Due to the lack of detailed underlying data in the ASIC report, BDO was unable to complete a like-for-like comparison between the UK and Australia from the reported values.



[11] Transactions whereby the victim involved initiates or facilitates the transaction, including under a false belief as to where and/or to whom the funds are going.

Comparing scam reporting

As previously identified, the approach to identifying, categorising and reporting scams differs across jurisdictions; not just globally but within Australia itself. This makes direct comparisons between jurisdictions challenging, and means direct analysis by individual scam type the most effective comparison.

In Australia, national scam data is currently compiled via the Australian Competition and Consumer Commission (ACCC) from various sources, including from Scamwatch, ReportCyber, IDCARE, the Australian Securities and Investments Commission (ASIC) and bank-reported data through the Australian Financial Crimes Exchange (AFCX). While steps are taken to address and remove duplication in reporting, there are still challenges with this approach. For example, Scamwatch reports are often simply reports of a scam, not necessarily a customer loss. By comparison, in the UK, national scam data is based on bank-reported scams and is limited to the scope of the CRM. Therefore, comparing the two jurisdictional approaches likely sees Australia over-reporting scam losses, and almost certainly sees the UK under-reporting scam losses given banks are only concerned with reports for APP's that meet the criteria of the CRM.

The following section outlines the differences in scam reporting between banks in Australia and the UK.

UK versus Australia – understanding the scam reporting differences

The table below demonstrates the significant differences in reporting of scams in Australia and the UK. While not an exhaustive list, the table outlines the main parameters demonstrating exclusions in UK reporting. According to Westpac's own data, scam reporting parameters used in Australia and which are not reported on in the UK, account for approximately two thirds (66.3%)[12] of all Australian losses. This indicates a significant proportion of scams which are being excluded from UK reporting, but being reported in Australia.

Reporting parameter	AU	UK
Fast Payment Service (UK) / New Payments Platform (AU)	✓	✓
Bank Clearing System (UK) / Direct Entry (BECS) (AU)	✓	x
PayPal	✓	x
Branch / Cash	✓	x
Crypto wallet transfers	✓	x
International Funds Transfer	✓	x
Businesses (bigger than sole trader)	✓	x
FX payments	✓	x
Scam loss cap[13]	✓	x
Statute of limitations[14]	✓	x

These parameters account for 66% AU losses

[12] This percentage has been calculated based on Westpac's own analysis and hasn't been verified by BDO

[13] Under CRM, losses only reported up to £85,000

[14] Under CRM, scams not reported if the loss occurred at least 13 months from time of reporting

Warranties and Disclaimers

BDO Services Pty Ltd is a member of an Australian association of independent accounting and management consulting firms trading under the name BDO.

BDO Services Pty Ltd conducts its business independently of all other firms of Chartered Accountants or other entities that trade under the name BDO.

BDO has prepared this report on the latest information available as at the date of this report. We accept no responsibility to update it for events that take place after the date of its issue.

In completing this report BDO has relied upon information provided, which we believed to be reliable, complete and accurate. Comments and observations are based on information provided at the time of writing the report. BDO reserves the right to amend or update this report if information not previously available, known or provided, becomes known after the date of issue of this report.

The engagement of BDO is as an independent contractor and not in any other capacity. We are not responsible for the appropriateness of any commercial or strategic decisions taken by any parties. We have assumed that the information provided to us in response to our requests is complete and accurate.

In preparing this report, BDO has referred to, considered and relied upon various sources of data, including data provided by Westpac. All data sources are referenced in an appendix to the report.

The publication, disclosure, or use of this report by any other party requires BDO's express consent in writing. The exceptions to this requirement are a disclosure to others within your organisation or your professional advisors on a confidential basis, or as required by law, court order or any regulatory or professional body as part of, or as a result of, our scope of work.

The services provided in connection with this engagement comprise an advisory engagement, which is not subject to assurance, or other standards issued by the Australian Auditing and Assurance Standards Board and, consequently no opinions or conclusions intended to convey assurance have been expressed. No warranty of completeness, accuracy or reliability is given in relation to the statements and representations made by, and the information and documentation provided.

Limitations

In conducting the data analysis a number of limitations were identified, including:

- Consistent Canadian data could not be identified for the requested period (2019 to 2024), instead analysis over Canadian data has been conducted from 2021 to 2024.
- Consistent Australian data could not be identified for the requested period (2019 to 2024), instead analysis over Australian data has been conducted from 2020 to 2024.
- Consistent USA data could not be identified for the requested period (2019 to 2024), instead analysis over USA data has been conducted from 2020 to 2024.
- Consistent UK data could not be identified for the requested period (2019 to 2024), instead analysis over UK data has been conducted from 2019 to 2023.
- Data has been collected from trusted government sources and may not represent the entire dataset for a jurisdiction (e.g. individuals may not report scams).
- All monetary figures from each jurisdiction have been converted to Australian Dollar. BDO notes this conversion may have caused exchange rate differences within the data.
- The Scamwatch data does not provide detailed data points for each transaction. Therefore, specific data exclusions were unable to be conducted when attempting to make the data like-for-like based on the UK model.

- BDO was unable to obtain specific Westpac scam data to ascertain the percentage amount each transaction type for exclusion (e.g. remote access scam, relates to Bitcoin, non-NPP network etc.) makes up within its overall scam data.

Appendices

Appendix 1 – Categorisation

In conducting the analysis, to ensure comparability across jurisdictions which record various scam types, scam types have been allocated to the following categories:

Category Name	United Kingdom	Australia	Canada	USA
Romance	Romance Scam	Dating and romance scams	Romance	
Investment	Investment Scam	Investment scams	Investments	Investment Related
		Pyramid schemes	Pyramid	
Remote Access	Mobile Banking Fraud	Phishing	Phishing	Internet Services
	Remote Purchase (CNP) Fraud	Ransomware and malware	Spear Phishing	
	Internet Banking Fraud	Remote access scams	Spoofing	
	Telephone Banking Fraud	Hacking	Telecom Fraud	Telephone and Mobile Services
			Modem-Hijacking	
Unexpected Winnings		Scratchie scams	Vacation	Travel, Vacations and Timeshare Plans
		Travel prize scams	Prize	Prizes, Sweepstakes and Lotteries
		Unexpected prize & lottery scams	Timeshare	
		Betting and sports investment scams	Survey	
		Travel, prizes and lottery scams		
Buying/Selling Scams	Purchase Scam	Online shopping scams	Office Supplies	Office Supplies and Services
	Invoice and Mandate Scam	False billing	False Billing	Online Shopping and Negative Reviews
		Fake charity scams	Charity / Donation	Charitable Solicitations

		Psychic and clairvoyant	Psychics	Magazines and Books
		Health and medical products	Health	Health Care
		Overpayment scams	Vendor Fraud	Internet Auction
		Mobile premium services	Service	Tax Preparers
		Classified scams	Counterfeit Merchandise	
			Merchandise	
			Directory	
Job and Payment Scams	Advance Fee Scam	inheritance and unexpected money	Foreign Money Offer	Foreign Money Offers and Fake Check Scams
	Cheque	Inheritance scams	Fraudulent Cheque	Advance Payments for Credit Services
		Rebate scams	Loan	Mortgage Foreclosure Relief and Debt Management
		Jobs and employment scams	Job	Business and Job Opportunities
			GRANT	Grants
Impersonation/ Threats	Impersonation: Other	Threats to life, arrest or other	Unauthorized Charge	Imposter Scams
	Impersonation: Police/Bank Staff		Bank Investigator	
	CEO Scam		Collection Agency	
			Recovery Pitch	
			Emergency (Jail, Accident, Hospital, Help)	
			Extortion	
Identity Theft	Card ID Theft	Identity theft	Identity Fraud	
			Personal Info	
	Counterfeit Card Fraud			

Other	Lost and Stolen Card Fraud			
		Other scams	Incomplete	
			Other	
			Unknown	

Appendix 2 – Glossary

Term	Definition
Romance Scam	Occurrence where a criminal adopts a fake online identity to gain a victim's affection or trust.
Investment scam	Occurs when a scammer attempts to 'trick' an individual into investing money.
Pyramid Scheme	A fraudulent system of making money through recruiting an ever-increasing number of 'investors'.
Mobile Banking Fraud	Involves malware-infected apps, fake banking apps, or even SIM card swapping to allow a scammer unauthorised access to an individual's mobile banking account.
Remote Purchase Fraud	Occurs when a scammer acquires an individual's card details
Internet Banking Fraud	The process of using technology to remove funds from an online bank account.
Telephone Banking Fraud	Targeted attempt to manipulate an individual to perform certain actions or divulging confidential information.
Phishing	Social engineering attached which is used to steal an individual's personal information/data.
Spear-phishing	An attempt to acquire sensitive information or access to a computer system through sending messages which appear legitimate to specific individuals (or organisations).
Spoofing	Occurrence where a scammer disguises an email address, name, phone number etc., to convince an individual they are interacting with a trusted source.
Ransomware	A type of malicious software that cybercriminals use to 'infect' electronic devices and networks to restrict access to data until a sum of money is paid.
Remote Access Scam	Occurs when individuals are contacted by a scammer falsely claiming to be from a familiar company, who request remote access to a personal device.

Modem-hijacking	Scammers accessing software on an individual's computer which causes the modem to dial phone numbers which incur telephone charges.
Scratchie Scam	Scammers provide fake scratch-off cards that promise a prize if the individual first pays a fee.
Travel Prize Scam	Scammer requests an individual pays money to claim a 'reward' such as a free or discounted holiday.
Betting and sports investment scams	A scammer will convince a victim to invest in a betting system or software
Timeshare scam	A scammer contacts a timeshare owner whilst assuming the identity of a reseller or real estate agent.
Survey Scam	A survey delivered via phone or online communication methods to gather personal information.
Purchase Scam	Occurrence where scammers set-up fake websites or profiles on actual retailer sites to officer products or services at low prices.
Invoice and Mandate Scam	Occurs when a scammer poses as a trusted organisation and provides an invoice with differing bank details.
Fake Charity Scam	Scammers act as a charity and collect money from individuals.
Psychic and clairvoyant Scams	Scammers approach individuals and claim to help with a curse or jinx or even claim to help to win prizes (e.g. lottery)
Health and medical products Scam	Products claim to prevent, treat or cure health conditions, but are not proven effective for those uses.
Overpayment Scams	A scammer falsely claiming to have sent a victim an excess of money.
Mobile Premium Services Scam	Scammers create SMS competitions or trivia scams to 'trick' an individual into paying call or text rates when replying to the message.
Classified Scam	Scammers pose as sellers, and post fake advertisements on classifieds websites
Counterfeit Merchandise Scam	Goods, often of poor quality, are made and sold under another's brand name without the brand owner's authorisation.
Directory Scam	Scammers request payment for advertising in internet directories that sound legitimate but are not well renowned.

Internet Auction Scam	The fraudulent advertisement of non-existent goods on auction sites.
Tax Preparers Scam	A tax preparer files a tax return without authorisation or changes the return without the individual's knowledge.
Advance Fee Scam	A scammer promises the victim a large sum of money, in return for a small up-front payment.
Cheque Scam	Where a fake cheque is presented to a business for the payment of goods or services.
Inheritance and Unexpected Money Scam	Scammers attempt to convince an individual they have won or inherited money, where to access the individual must provide banking details and an upfront fee.
Rebate Scams	A scammer acts like a government organisation and claims and individual us owed a rebate
Job and Employment Scam	A scammer deceives an individual into providing funds by offering a 'guaranteed' way obtain a high-paying job.
Foreign Money Offer Scam	A scheme used to defraud traders through convincing them to expect to gain a high profit through trading on the foreign exchange market.
Loan Scam	A scammer makes large promises which cannot be delivered and hides fees in the loan.
Impersonation scams	A scammer claims to be from a trusted organisation who threatens an individual into handing over money or personal information.
Unauthorised Charge Scam	Where funds are transferred from an individual's account without permission.
Bank Investigator Scam	A scammer attempts to convince a victim to disclose banking information to then use the information to remotely access the victim's account.
Recovery Pitch Scam	A scammer targets a scam victim and prvides a promise to recover their lost funds for a fee.
Identity Theft	Involves using an individual's identity to steal personal information, money or other benefits.
Card not Received Scam	Occurs where a bank card is stolen while in transit to an individual.

Counterfeit Card Fraud	Where a fraudster counterfeit or clone an individual's card with their knowledge.

Appendix 3 – Collection of Data

The publicly available data utilised for analysis was taken from the following government run agencies:

Jurisdiction	Government Agency	Agency Responsibilities	Link
Australia	ACCC (National Anti-Scam Centre)	The National Anti-Scam Centre works across both the government and private sector to protect Australians from scam and provide a scam reporting system.	National Anti-Scam Centre
United Kingdom	UK Finance	UK Finance publish fraud and scam data provided from financial providers, credit, debit and charge card issuers, and card payment acquirers.	UK Finance
Canada	Canadian Anti-Fraud Centre	The Canadian Anti-Fraud Centre collects information on fraud and identity theft. To provide information on past and current scams affecting Canadians.	Canadian Anti-Fraud Centre
United States of America	Federal Trade Commission	The Federal Trade Commission aims to provide protection to the public from deceptive and unfair business practices and provides a scam reporting system.	Federal Trade Commission

Appendix 4 – APP Categorisations

The following scam types recorded for each jurisdiction have been used in the analysis of APP scam data:

UK	Australia	Canada	USA
Purchase Scam	Dating and romance scams	Romance	Investment Related
Investment Scam	Investment scams	Investments	Office Supplies and Services
Romance Scam	Online shopping scams	Office Supplies	Online Shopping and Negative Reviews
Advance Fee Scam	False billing	False Billing	Charitable Solicitations
Invoice and Mandate Scam	Fake charity scams	Charity / Donation	Magazines and Books
CEO Scam	Psychic and clairvoyant	Psychics	Health Care
Impersonation: Police/Bank Staff	Health and medical products	Health	Internet Auction
Impersonation: Other	Overpayment scams	Vendor Fraud	Tax Preparers
	Mobile premium services	Service	Foreign Money Offers and Fake Check Scams
	Classified scams	Counterfeit Merchandise	Advance Payments for Credit Services
	inheritance and unexpected money	Merchandise	Mortgage Foreclosure Relief and Debt Management
	Inheritance scams	Directory	Business and Job Opportunities
	Rebate scams	Foreign Money Offer	Grants
	Jobs and employment scams	Loan	Imposter Scams
	Threats to life, arrest or other	Job	
		GRANT	
		Unauthorized Charge	
		Bank Investigator	
		Collection Agency	
		Recovery Pitch	
		Emergency (Jail, Accident, Hospital, Help)	
		Extortion	

1300 138 991

www.bdo.com.au

AUDIT • TAX • ADVISORY

NEW SOUTH WALES
NORTHERN TERRITORY
QUEENSLAND
SOUTH AUSTRALIA
TASMANIA
VICTORIA
WESTERN AUSTRALIA