



Award Winner

The Demographic Divide: An Analysis of Canadian Fraud Loss Patterns

Michael Kummer, BA

Any views and ideas expressed in the essay are the author's alone and may not reflect the views and ideas of the Society of Actuaries, the Society of Actuaries Research Institute, Society of Actuaries members, nor the author's employer.

ABSTRACT

Canadians are subject to various frauds and scams, with the dollars lost per scam influenced by an individual's senior status and gender. In the face of increasing automation, exploring current vulnerabilities to undermine scam innovation is critical. Results indicate that seniors tend to lose more money per scam than non-seniors, especially when scammers use a more personable method. Males are most vulnerable to investment scams while females are most vulnerable to romance scams. Professionals, such as financial planners, senior association management, and insurance managers, should implement creative intervention strategies to assist in scam prevention.

INTRODUCTION

An analysis of Canadian scams reveals that the category of the scam, the method used, and the demographic of the victim are related to the dollars lost per scam. A complete analysis becomes even more critical as the current scam and fraud landscape undergoes rapid innovation. Scammers are more successful with specific demographics depending on the type of scam committed and the medium used. As machine learning and large language models become more accessible, some scams are at risk of increasing automation. Engaging with the current scam and fraud landscape is critical to ensure that guardrails are pre-emptively implemented.

Analyzing the current landscape can assist with understanding if prior American research can be applied to Canada while also giving a picture of Canada's unique vulnerabilities. The Canadian Anti-Fraud Centre Fraud Reporting System Dataset will be used to determine precisely what broad effects gender and senior status have on scam efficacy. Based on the correlations between dollars lost and victim gender/senior status, specific scam types and methods were found to vary in their financial impact. All significant scams and methods cause individuals to lose more if the scams are more personal but vary in impact depending on gender and senior status. The effect on each demographic varies, as some scams will impact seniors drastically differently from non-seniors, with differences between males and females also varying.

BACKGROUND

Seniors in Canada have experienced a vast lifestyle change due to COVID-19, as they have become more online and increasingly isolated. Seniors over 75 have experienced a 10% jump in internet usage between 2020 and 2022.¹ During COVID, many non-profits and volunteer-run religious organizations vanished.² Many communities that rely on volunteers and non-profits can no longer be supported by volunteering seniors, and those seniors who want to volunteer cannot, so they are left unable to and without the social network they would have otherwise had. This combination has led to an unfortunate situation where seniors have less community support and are more online.

Every scam can have varying impacts on the victim, and even though fraud might have a significant blow to the individual's life, the incident might not lead to any direct monetary loss. Some scams require a prior successful scam on the same victim, as the scammers require preceding information to defraud a victim. These grey areas make assigning dollars lost to scams difficult to assess as the exact dollar value of stolen personal information is difficult to quantify, and multiple scams can build off one another. For example, Canada's Anti-Fraud Centre Fraud Reporting System Dataset contains information on over 320,000 successful and unsuccessful scams within Canada. Notably, the dataset has many victims reporting a dollar loss of \$0 as the losses might have been absorbed by their workplace, or the crime might have preceded another scam where there was a monetary loss.³

METHODOLOGY

The following OLS regression was done on categorical data from Canada's Anti-Fraud Centre Fraud Reporting System Dataset. As of April 2025, the dataset contains observations from January 2020 to March 2025, totaling around 324,000 observations. Data where information is anonymized, N/A, data where losses were 0, and non-victim data was excluded. The rationale is that non-zero losses do not necessarily mean they are not zero and may be extremely hard to quantify. For overly anonymized data, there are inherent difficulties with analyzing N/As.

$$\text{Analysis Data} = \text{Victim} \cap \text{Non-Zero Loss} \cap \text{Not Anonymized} \cap \text{Not Missing}$$

Small categories with few observations were combined or removed. For the methodology used, mail, television, video call, print, and radio were combined into an "other" category as these methods ranged from 80 to three observations in respective order. For scam categories, those below 200 observations were combined as the number of observations becomes a limitation to understanding their representation of the greater Canadian population.

¹ Statistics Canada. "Canadian seniors more connected than ever." *StatsCAN Plus*, August 14, 2023, accessed April 10, 2025, <https://www.statcan.gc.ca/o1/en/plus/4288-canadian-seniors-more-connected-ever>

² Don McRae. "Volunteer-Supporting Charities Are Closing at Alarming Rates." *PANL Perspectives*, Carleton University, August 22, 2023, <https://carleton.ca/panl/2023/volunteer-charities-close-at-alarming-rates/>.

³ Royal Canadian Mounted Police. "Description and Associated Definitions of Canadian Anti-Fraud Centre (CAFC) Statistics" (Ottawa: Royal Canadian Mounted Police, n.d.), 4.

Figure 1

COMPARISON BETWEEN THE TOP SIX SCAMS IN FREQUENCY AND THEIR RESPECTIVE DOLLAR LOSS FOR SENIORS VS. NON-SENIORS

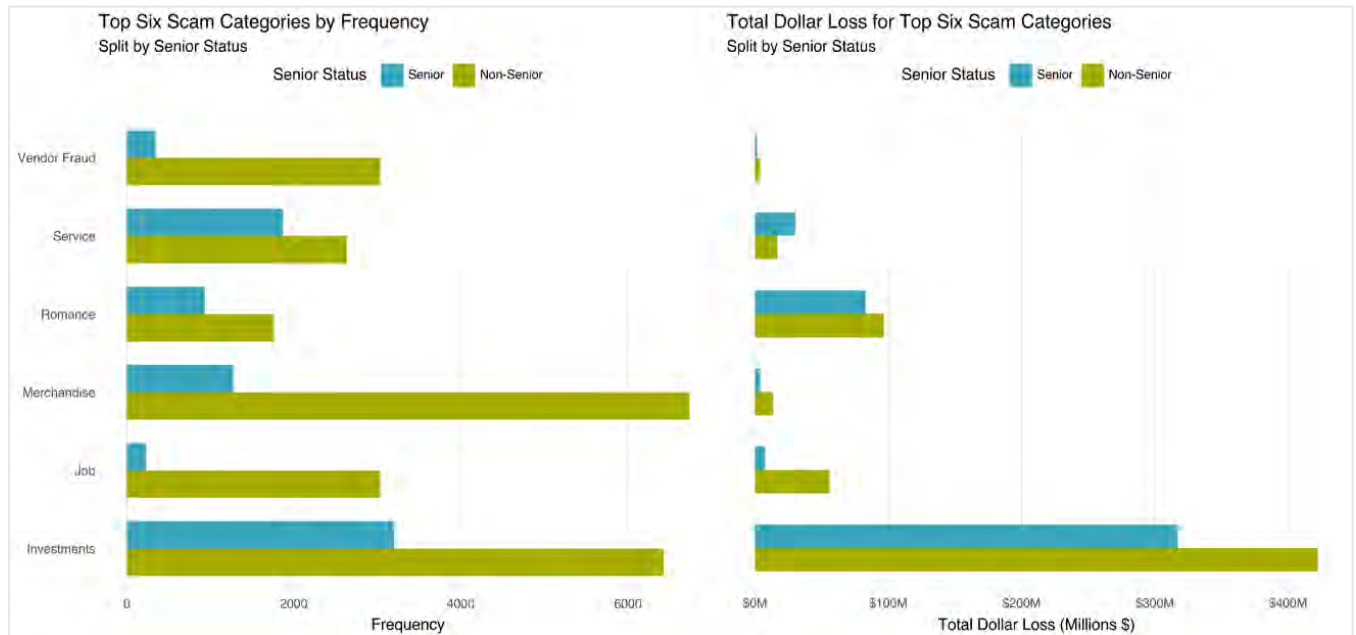
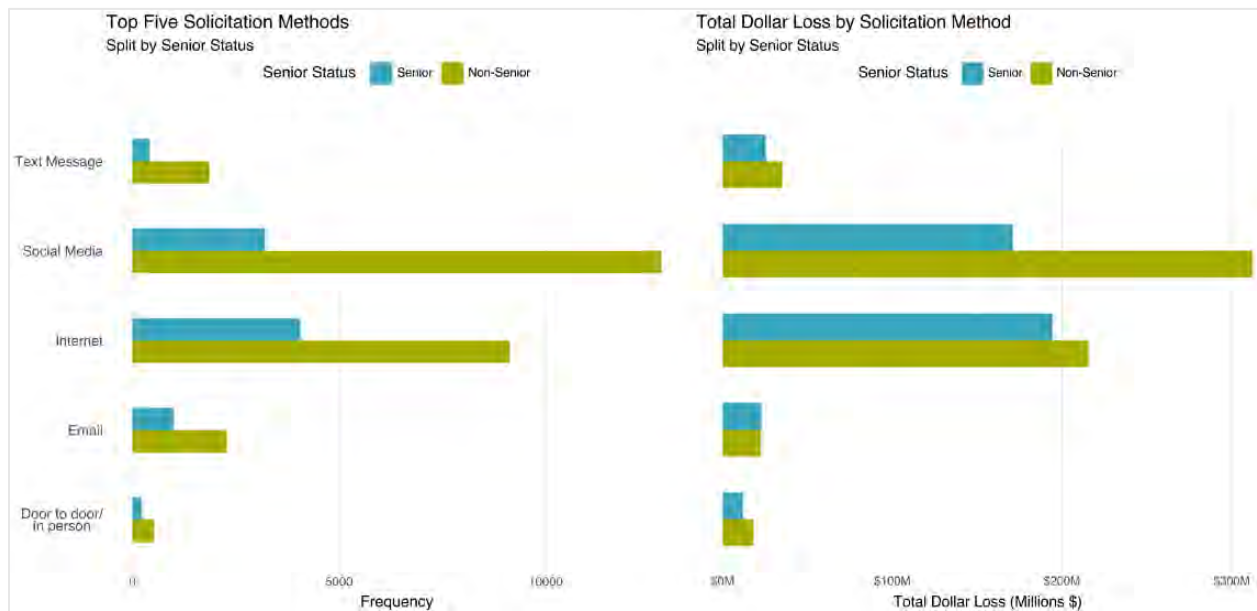


Figure 2

COMPARISON BETWEEN THE TOP FIVE METHODS IN FREQUENCY AND THEIR RESPECTIVE DOLLAR LOSS FOR SENIORS VS. NON-SENIORS



MODELS

Category Interaction:

$$\ln(DollarLoss_i) = \beta_0 + \sum_j \beta_j Category_{ij} + \beta_{gender} Gender_i + \beta_{senior} Senior_i + \beta_{year} Year_i + \sum_k \beta_k SolicitMethod_{ik} \\ + \sum_j \beta_{j,s}(Category_{ij} \times Senior_i) + \sum_j \beta_{j,g}(Category_{ij} \times Gender_i) + \varepsilon_i$$

An OLS regression will determine each variable's impact, and multiple models will be used to ensure that interactions between solicitation methods, gender, location, and year will be discernable. The natural log of the dollar loss amount was used due to the extremely wide range between the minimum and maximum values. Non-seniors were a reference category due to the abundance of observations, and non-seniors were more evenly spread across the scams. Overall, the gender demographics were split equally except for a few scams, meaning it does not have any significance what gender the reference category is. The reference year was chosen to be 2020 as it is the first year of observations.

The reference categories and methods were chosen due to their size and comparability. The reference category chosen was Emergency Fraud, where the scammer pretends to be someone the victim knows and urgently requests money for bail, a hospital bill, etc. Emergency fraud has varied solicitation methods and typically requires some information about the victim but does not require the scammer to build a relationship with them. Direct Call/Phone was chosen as the reference category for the solicitation methods due to the ability to do various scams over the phone. Alongside the observation counts, phone and direct call scams can be automated or done manually.

Much of the data contained categories with an even spread. Gender was relatively evenly split between males and females. There was near-normal distribution for the ages. Scams and solicitation methods contained few categories with many observations and some categories with very few observations.

ROBUSTNESS CHECK

Due to the abundance of interaction terms, multicollinearity and homoskedasticity become problematic as the interaction terms start to predict each other. As a robustness check, values under 100, 500, and 1,000 and those above 25,000, 50,000, and 100,000 were dropped. Removing either bound drastically decreases the R^2 to the 0.15 to 0.25 range, while removing both only minorly decreases the R^2 to around 0.3, meaning the extremes add explanatory power to the model. Multicollinearity and heteroskedasticity also become problematic with this many interaction terms. The basic and male/senior interaction models do not suffer from the term amount issues, but these models are only capable of an extremely simplified view. Methods to penalize specific interactions could be implemented on top of a simple demographic model, creating a more technically robust but more complex model.

DATA

Table 1

DEMOGRAPHICS

Variable	Basic	Male/Senior Interaction	Solicit Interaction	Category Interaction
Intercept	7.821***	7.814***	7.823***	7.266***
Male	0.084***	0.092***	-0.059	-0.044
Senior	0.301***	0.314***	0.396***	0.999***
Year	0.164***	0.164***	0.164***	0.164***
Adjusted R ²	0.424	0.424	0.424	0.431

Note: The table's reference category is Emergency Fraud, and the reference solicit method is direct call.

*p<0.1; **p<0.05; ***p<0.01

Table 2

SCAM CATEGORY VULNERABILITY PROFILE

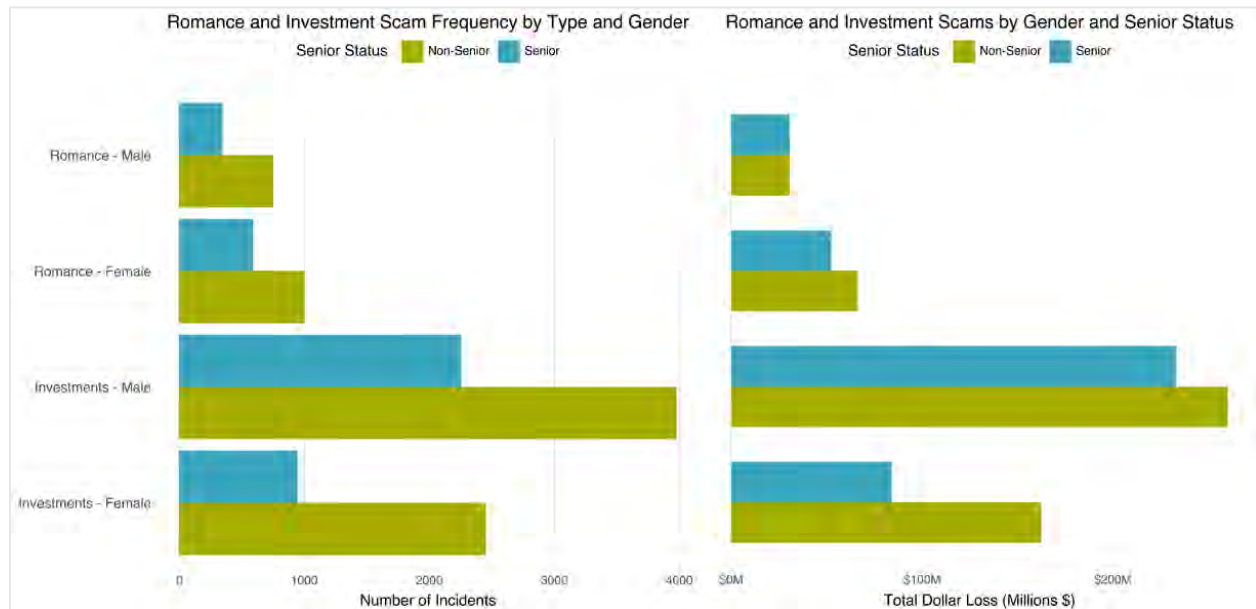
Scam & Interaction Term	Basic	Male/Senior Interaction	Solicit Interaction	Category Interaction
Recovery Pitch	0.771***	0.774***	0.789***	0.998***
Recovery Pitch X Male				0.364**
Recovery Pitch X Senior				-0.468**
Investment	1.925***	1.928***	1.935***	2.317***
Investment X Male				0.251**
Investment X Senior				-0.735***
Extortion	0.033	0.035	0.058	1.090***
Extortion X Male				-0.947***
Extortion X Senior				-0.439***
Romance	1.958***	1.960***	1.968***	2.525***
Romance X Male				-0.509***
Romance X Senior				-0.303**

Note: The table's reference category is Emergency Fraud, and the reference solicit method is direct call.

*p<0.1; **p<0.05; ***p<0.01

Figure 3

COMPARISON OF FREQUENCY OF GENDER AND SENIORITY STATUS IN INVESTMENT AND ROMANCE SCAMS



For romance scams, females will lose more than males, especially females who are non-seniors. Previous American research aligns with this, but specific research has shown that educated women who score high in risk-taking are specifically the most vulnerable to this type of scam.⁴ Results here show that females were both scammed for more money and more frequently than males. Women who are not seniors are scammed more often, but senior women are scammed for more money per scam.

Male victims to lose more to Investment and recovery scams, with senior males losing more per scam but less collectively. There is detailed American research on investment scams, with the exact demographics being individuals who are not financially destitute and willing to engage in risky behavior.⁵ The study suggests that the desire to gain wealth is driving male individuals to seek out unregulated investing areas.⁶

⁴ Monica T. Whitty. "Do You Love Me? Psychological Characteristics of Romance Scam Victims." *Cyberpsychology, Behavior and Social Networking* 21, no. 2 (February 1, 2018): 105-109, <https://doi.org/10.1089/cyber.2016.0729>.

⁵ Marguerite DeLiema, Doug Shadel, and Karla Pak. "Profiling Victims of Investment Fraud: Mindsets and Risky Behaviors." *Journal of Consumer Research* 46, no. 5 (2020): 904-914, <https://doi.org/10.1093/jcr/ucz020>.

⁶ *ibid*, 911.

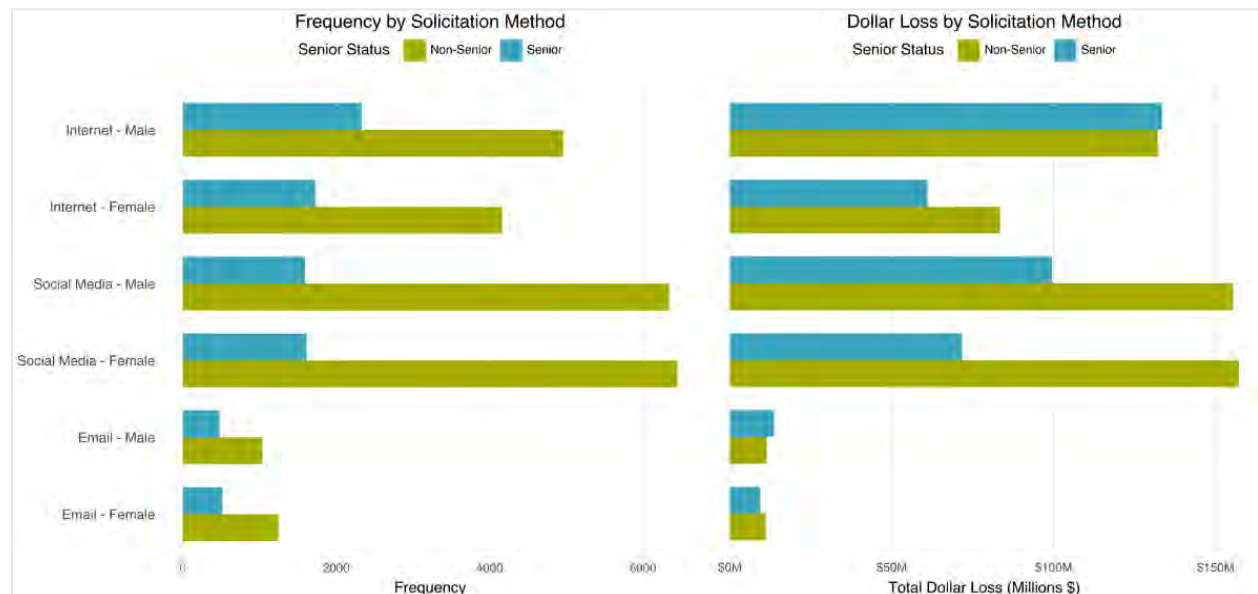
Table 3
METHOD VULNERABILITY PROFILE

Method & Interaction Term	Basic	Male/Senior Interaction	Solicit Interaction	Category Interaction
Email	-0.676***	-0.676***	-0.799***	-0.581***
Email X Male			0.470***	
Email X Senior			-0.227***	
Internet	-0.592***	-0.591***	-0.632***	-0.499***
Internet X Male			0.205***	
Internet X Senior			-0.114**	
Social Media	-0.722***	-0.722***	-0.712***	-0.607***
Social Media X Male			0.107**	
Social Media X Senior			-0.108*	
Text Message	-0.324***	-0.325***	-0.215***	-0.226***
Text Message X Male			0.008	
Text Message X Senior			-0.326***	

Note: The table's reference category is Emergency Fraud, and the reference solicitation method is direct call. Other was significant, but Other X Male and Other X Senior were not.

*p<0.1; **p<0.05; ***p<0.01

Figure 4
COMPARISON OF GENDER AND SENIORITY STATUS FOR EMAIL, INTERNET, AND SOCIAL MEDIA SCAMS



A breakdown of methodologies shows that some methods are gendered, but there are more pronounced differences between seniors and non-seniors. The seniority difference is stark in that seniors are scammed fewer

times online, but they lose a substantially larger amount per scam. This suggests that seniors are more *susceptible* and non-senior are more *accessible* to scams using online mediums.

EMPIRICAL ANALYSIS AND EXPLANATION

Scams being gendered in their impacts means that the type of language used within the scams should be investigated. Seeing what exactly is enticing for each gender or age category can potentially allow us to mitigate the most significant contributing factors to being scammed. Since personal solicitation methods are more effective than those where the person on the other end is unknown, the risk from automated scams appears to be relatively low. Protecting seniors online needs to become a priority as they are losing more per scam that might be easily preventable. Still, it is only a matter of time until scammers use machine learning to augment personal scams.

The correlations between dollar loss and gendered scams or scams that focus on seniors varies. Some scams are quite successful with specific demographics, leading to the belief that there is something intrinsic about these scams and demographics. Specific methods where the victim is unknown, such as text messages, seem indiscriminate in who they target and have no significant demographic differences. In comparison, email is also indiscriminate, yet something specific about males and non-seniors causes them to lose more money over email. This contrast might be explained by the perception of emails versus text messages. For example, a fake login portal bank notification or e-transfer may seem more legitimate over email than text, but more research is needed to find potential reasons for why this difference exists.

A significant limitation is that we cannot see further details about each occurrence. Since so many unsuccessful attempts exist, follow-up research should be conducted on attempts and observations with a loss of \$0. As mentioned, the category amounts in this model are cumbersome, so a more technically robust lasso regression or other penalized method could better explain the current trends seen, especially when focusing on only larger or smaller losses. The dataset is also updated frequently, so predictive analysis is possible as multiple times a year, there are more observations to test models on.

CONCLUSION AND RECOMMENDATIONS

As seniors become more online and have less social support, their susceptibility to being scammed for large sums of money becomes a critical concern. Retirement organizations such as teacher associations and advocacy groups should ensure seniors understand potential scam techniques. Synthetic voice scam calls could be prevented entirely if seniors were taught to call the individual requesting money to ensure it is genuinely them and not a spoofed call. Suppose the individual is calling from potentially a hospital or courthouse; in most realistic situations, the transfer of funds can wait until the senior is at the location and can verify it is true, especially as they would most likely go to that location anyway.

More research must be conducted on what exactly makes some scams gendered and more damaging to seniors. The study on romance scams shows that risk-taking behavior is inherently intertwined with romance scam susceptibility. The investment scam study shows that, most likely, individuals scammed by fake investments were looking for grey areas to gain money. How to use this information to help prevent scams is quite complex and will most likely have to be tailor-made.

Due to the unique nature of some scams and the rapid advancements currently being made, creative measures should be implemented for each scam category, and preventing initial contact should be a focus for all scams. The landscape for scams is constantly changing, and scammers will improve in both their skills and techniques over time. The dangers of automated scams will likely have to be met with more automation. Scams requiring prolonged contact cannot be fully automated, but as automation techniques become more impressive, protecting some victims from themselves will become increasingly challenging.

REFERENCES

- DeLiema, Marguerite, Doug Shadel, and Karla Pak. "Profiling Victims of Investment Fraud: Mindsets and Risky Behaviors." *Journal of Consumer Research* 46, no. 5 (2020): 904-914. <https://doi.org/10.1093/jcr/ucz020>.
- Canadian Securities Administrators. "Common Frauds and Scams." Canadian Securities Administrators (website). Accessed April 4, 2025. <https://www.securities-administrators.ca/investor-tools/avoiding-fraud/common-frauds-and-scams/>.
- McRae, Don. "Volunteer-Supporting Charities Are Closing at Alarming Rates." *PANL Perspectives*, Carleton University, August 22, 2023. <https://carleton.ca/panl/2023/volunteer-charities-close-at-alarming-rates/>.
- Royal Canadian Mounted Police, Canadian Anti-Fraud Centre. "Canadian Anti-Fraud Centre Fraud Reporting System Dataset." Open Government, Government of Canada. Published July 10, 2023, modified April 1, 2025. <https://open.canada.ca/data/en/dataset/6a09c998-cddb-4a22-beff-4dca67ab892f>.
- Statistics Canada. "Canadian seniors more connected than ever." *StatsCAN Plus*. August 14, 2023. <https://www.statcan.gc.ca/o1/en/plus/4288-canadian-seniors-more-connected-ever>. Accessed April 10, 2025.
- Whitty, Monica T. "Do You Love Me? Psychological Characteristics of Romance Scam Victims." *Cyberpsychology, Behavior and Social Networking* 21, no. 2 (February 1, 2018): 105-109. <https://doi.org/10.1089/cyber.2016.0729>.

APPENDIX

ALL MODELS:

Model 1: Base Vulnerability Model:

$$\ln(\text{DollarLoss}_i) = \beta_0 + \sum_j \beta_j \text{Category}_{ij} + \beta_{\text{gender}} \text{Gender}_{\text{Male}} + \beta_{\text{senior}} \text{Senior}_i + \sum_k \beta_k \text{SolicitMethod}_{ik} + \beta_{\text{year}} \text{Year}_i + \varepsilon_i$$

Model 2: Male-Senior Interaction:

$$\ln(\text{DollarLoss}_i) = \beta_0 + \sum_j \beta_j \text{Category}_{ij} + \beta_{\text{gender}} \text{Gender}_i + \beta_{\text{senior}} \text{Senior}_i + \beta_{g \times s} (\text{Gender}_i \times \text{Senior}_i) + \sum_k \beta_k \text{SolicitMethod}_{ik} + \beta_{\text{year}} \text{Year}_i + \varepsilon_i$$

Model 3: Solicitation Interaction:

$$\ln(\text{DollarLoss}_i) = \beta_0 + \sum_j \beta_j \text{Category}_{ij} + \beta_{\text{gender}} \text{Gender}_i + \beta_{\text{senior}} \text{Senior}_i + \beta_{\text{year}} \text{Year}_i + \sum_k \beta_k \text{SolicitMethod}_{ik} + \sum_{k,s} \beta_{k,s} (\text{SolicitMethod}_{ik} \times \text{Senior}_i) + \sum_{k,g} \beta_{k,g} (\text{SolicitMethod}_{ik} \times \text{Gender}_i) + \varepsilon_i$$

Note: Model 4 is the main model and is represented in the Methodology subsection, Models.

ANALYSIS DATA DESCRIPTION:

Table A.1

SOLICITATION METHODS

Solicitation Method	Count
Social Media	15,991
Internet	13,184
Direct Call	7,282
Email	3,275
Text Message	2,270
Door to Door/In Person	749
Other	168

Table A.2

SCAM/FRAUD CATEGORY

Category	Count
Investments	9,632
Merchandise	8,012
Service	4,507
Vendor Fraud	3,387
Job	3,264
Romance	2,698
Bank Investigator	2,213
Counterfeit Merchandise	1,885
Extortion	1,662
Emergency	1,654
Other	840
Spear Phishing	814
Loan	719
Prize	648
Recovery Pitch	518
Grant	366

Table A.3

AGE BREAKDOWN

Age Group	Count
1 - 20	1,360
20 - 29	7,430
30 - 39	7,042
40 - 49	6,357
50 - 59	5,945
60 - 69	6,318
70 - 79	4,045
80 - 89	1,250
90+	164


Table A.4

GENDER BREAKDOWN

Gender	Count
Male	21,618
Female	21,201

* * * * *

Michael Kummer, BA, holds a degree in Psychology and History with nonprofit experience addressing issues affecting senior volunteers. He is currently completing an after- degree in Economics with a minor in Computer Science. He can be reached at mkummer@ualberta.ca.



Give us your feedback!
Take a short survey on this report.

[Click Here](#)

