SINGAPORE POLICE FORCE
SAFEGUARDING EVERY DAY

Investing in Love: Behavioural Analysis of Investment Scams

Project Team:
Carolyn Misir
Principal Psychologist

Tan Wei LIang
Psychologist

Dr. Jansen Ang
Director

Police Psychological Services Department

22 November 2024

Caveat

- The views expressed in this presentation are the author's only and do not represent directly or imply any official policy position or view of the Singapore Police Force or Ministry of Home Affairs
- No materials may be reproduced or stored electronically or in print without written permission from the Police Psychological Services Department

Scope of Presentation

1. Background
2. Research Question
2. Literature Review
3. Methodology
4. Findings
6. Crime Prevention Strategies
7. Limitations

1. Background

Investment scams in Singapore

SPF (2024)

Top 10 Scam Types in Singapore
(Based on number of reported cases)

Types of Scams	Cases reported		Total amount lost (at least)		Average amount lost in first half of 2024
	Jan - Jun 2024	Jan - Jun 2023	Jan - Jun 2024	Jan -Jun 2023	
E-commerce Scams	7,250	4,496	$8.6M	$7.3M	$1,191
Job Scams	5,717	5,723	$86.0M	$78.3M	$15,055
Phishing Scams	3,447	2,948	$13.3M	$7.3M	$3,868
Investment Scams	3,330	1,577	$133.4M	$80.4M	$40,080
Fake Friend Call Scams	2,368	3,832	$8.1M	$12.9M	$3,426
Government Officials Impersonation Scams	580	367	$67.5M	$40.4M	$116,534
Loan Scams	571	426	$2.5M	$2.5M	$4,459
Internet Love Scams	418	435	$12.5M	$25.7M	$29,969
Offer Sexual Services Scams	410	168	$1.9M	$439K	$4,780
Social Media Impersonation Scams	347	508	$1.8M	$4.4M	$5,454
Top 10 scams	**24,438**	**20,480**	**$336.1M**	**$260.2M**	**$13,754**

Note: Total amount cheated may not tally due to rounding.

- **Investment scams are 1 of the top 5 scam concerns**
- Highest increase in amount lost in 2024 compared to cases in 2023
- Highest total amount lost amongst scam types, at least $133.4million, in the first half of 2024

2. Research Questions

Research Questions

1. Why do people fall prey to investment scams?
2. How can we prevent people from falling prey to investment scams?

- There is a need to understand and contextualise the psychology of investment or economic crime scams for the localized context
- While the scam manifestations may be different across countries, identifying the underlying drivers of investment scam may inform us on countering the threat of scams and reducing the risk to victims

3. Literature Review

Dual-Process Models

Theoretical Framework for Judgement and Decision-making

System 1 & System 2

Kahneman (2011)

- Differentiation between two modes of thought and decisions are often based on mental S1 shortcuts driven by heuristics and biases
- Both systems do not function independently: Ideally, S2 should suppress and overrule S1. However, S1 can unconsciously encroach S2 due to its speed and efficiency, leading to decision errors

System 1
'Thinking Fast'

- Highly associative, involving "best guess"
- Automatic, quick, little to no effort
- Susceptible to biases and lead to irrational behavior

System 2
'Thinking Slow'

- Rule-governed and highly reflective
- Slow, conscious, controlled, effortful
- Requires attention and high-effort for logic and reasoning

Dual-Process Models

Theoretical Framework for Judgement and Decision-making

Elaboration Likelihood Model (ELM)

Petty & Cacioppo (1986)

- Attitudes are changed via two routes of persuasion following the Dual-Process model:
- Useful for scam psychology (Whitty, 2013)
  - Scammers leverage peripheral route, eliciting strong visceral influences that cause victims not to attend to cognitive cues causing decision errors

Peripheral Route

Susceptible to heuristics and biases that does not involve much elaboration

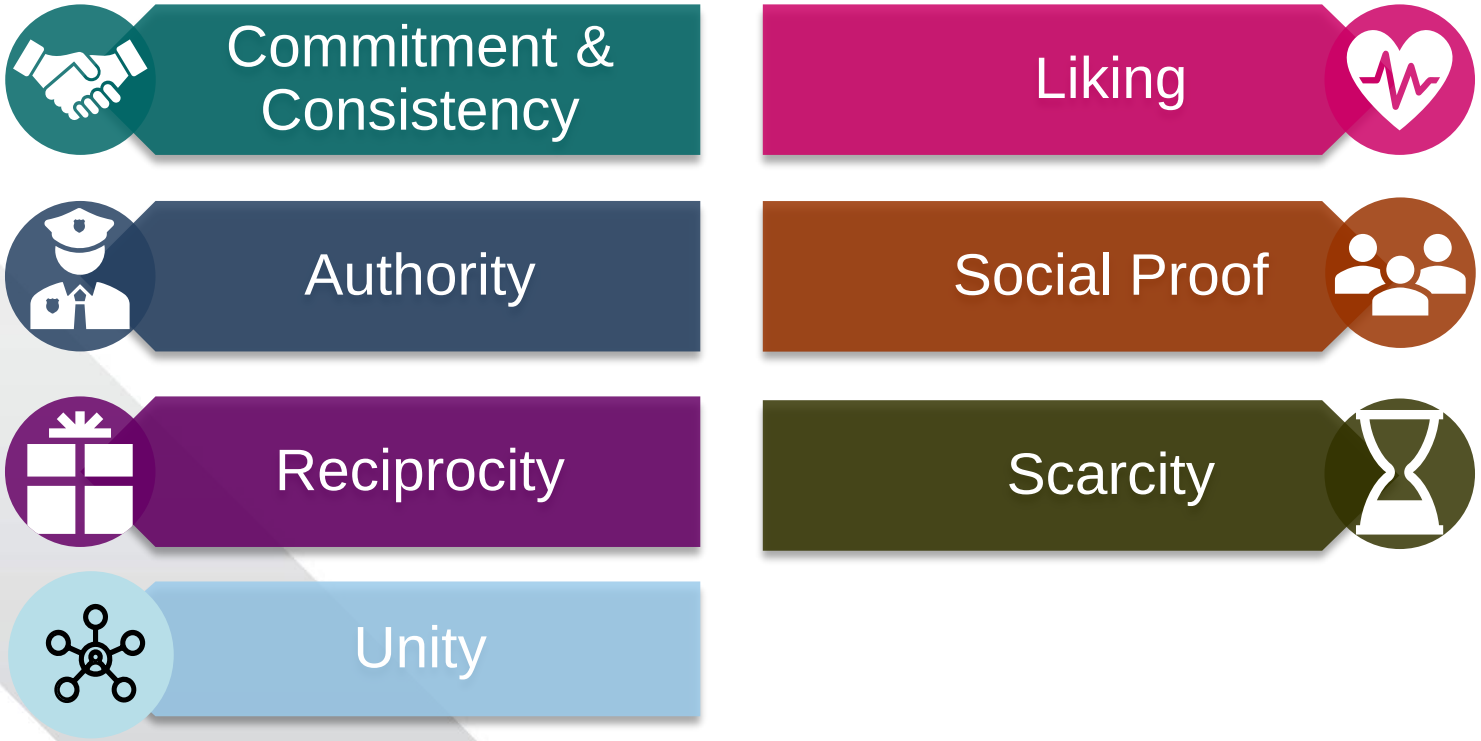
- Superficial information processing
- Reliance on peripheral cues
- Lack motivation or ability to use adequate cognitive resources

Central Route

Effortful thought that promotes high elaboration

- Deep information processing
- Motivated and able to employ adequate cognitive resources for systematic and critical thinking

Persuasion techniques in scam compliance



Cialdini, 1984, 2007, Langenderfer & Shimp, 2001; Rusch, 1999

Factors influencing scam compliance

Lea et al. (2009)

Visceral processes (Emotional triggers)

Strong motivations that elicit 'viscerally-oriented' rewards

- Scam messaging that use rich narratives appealing to emotions like greed, guilt, heroism, and charity such as the 'rags-to-riches' trope or helping someone in need (Fischer et al., 2013)
- Conditions of high visceral influence reduce motivation and likelihood of attending to scam-related cues in a message
- Reduce rational thought during decision-making (Langenderfer & Shimp, 2001)
- In strong motivational states, people tend not to elaborate on their decisions and neglect long-term consequences of the short-term rewards

4. Methodology

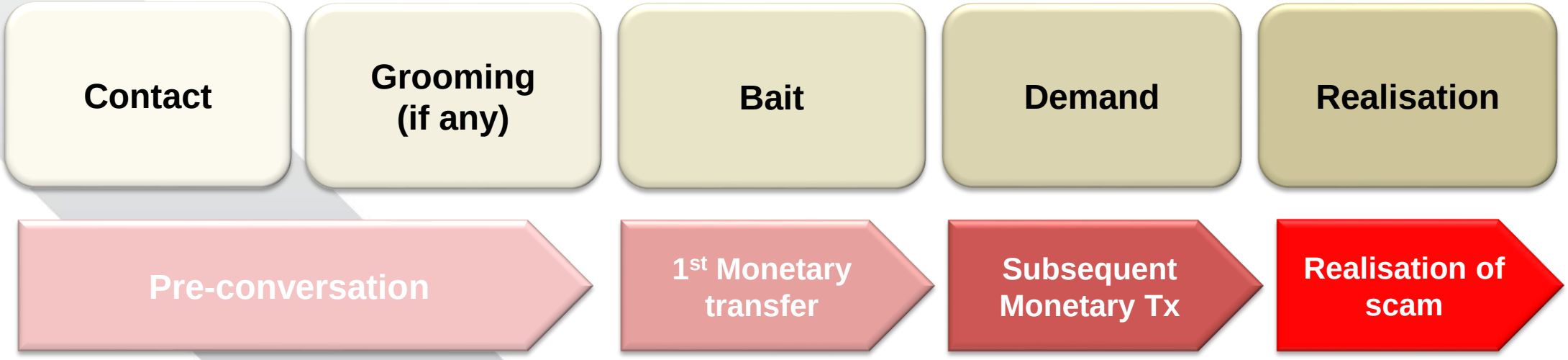
Methodology

- Mixed methods design
- Quantitative analysis of N= 270 statements of facts from victims of investment scam
- Qualitative analysis of in-depth interviews of investment scam victims

5. Findings

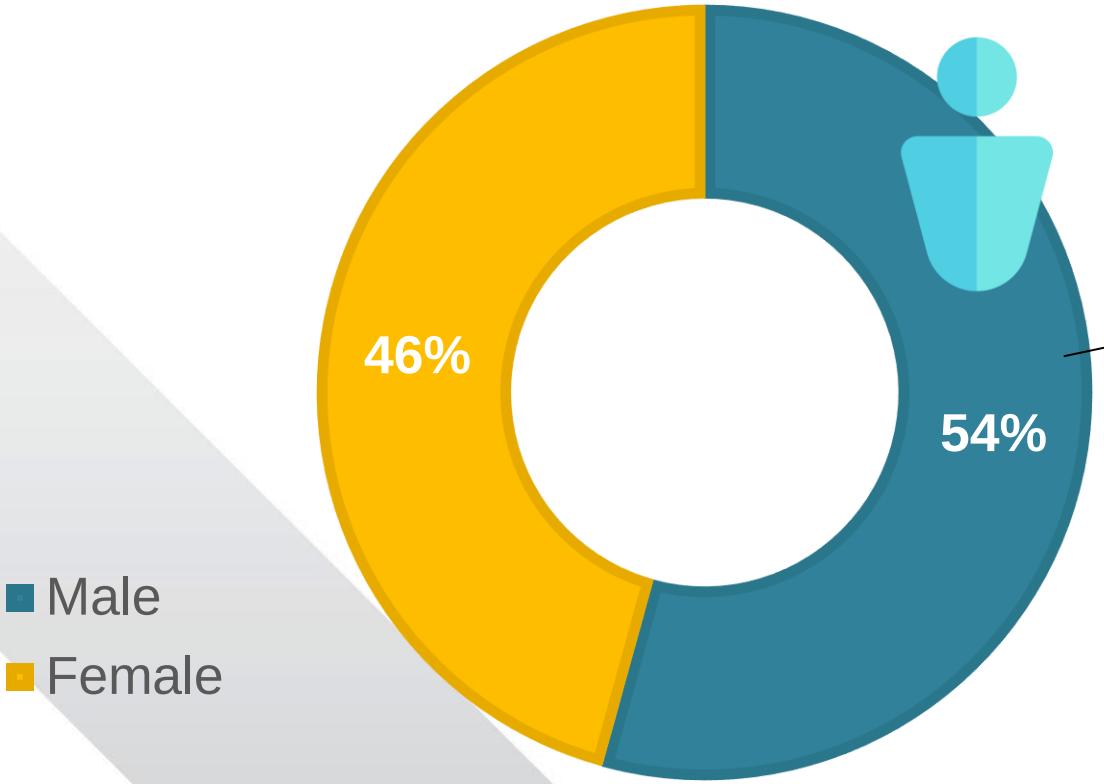
Process of Investment Scam

- Based on the modus operandi of investment scams in Singapore, the process of most scams follows this trajectory of events
- Some scams have a grooming element present
- This is either in terms of befriending the victims or in terms of establishing a romantic relationship with the victim before introducing the 'investment'



General Demographic Information

- Gender distribution of Responses (*N*=269)

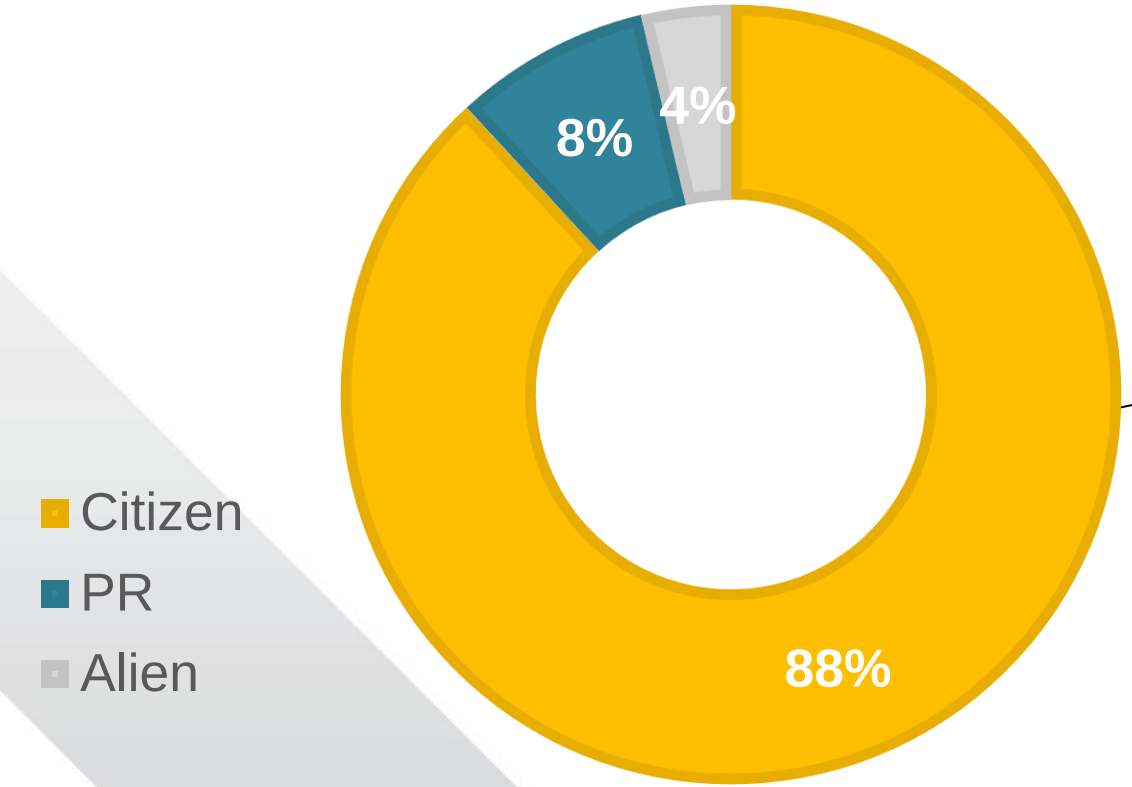


54% of victims are males,
which makes up majority of investment scam victims

Pre-Conversation | First Monetary Transfer | Sub. Monetary Transfer | Realisation

General Demographic Information

Citizenship of Victims (*N*=270)

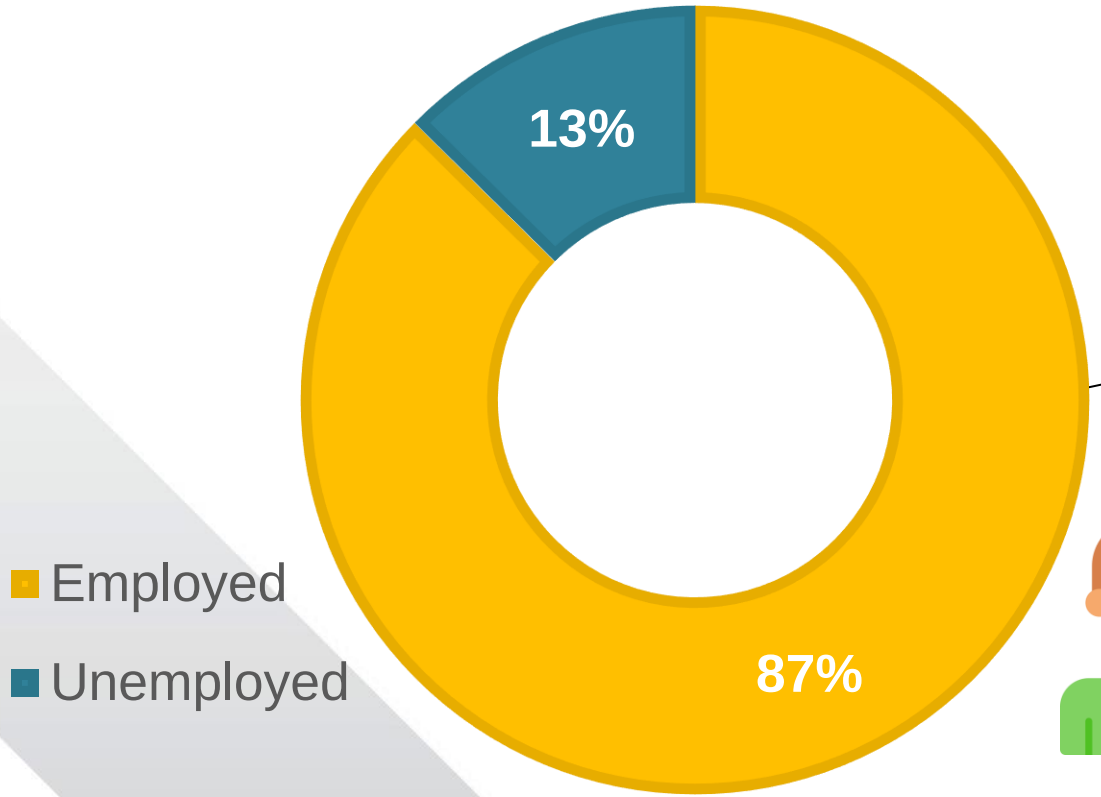


88% of victims are Singapore citizens

Pre-Conversation | First Monetary Transfer | Sub. Monetary Transfer | Realisation

General Demographic Information

- Occupation of Victims (*N*=270)

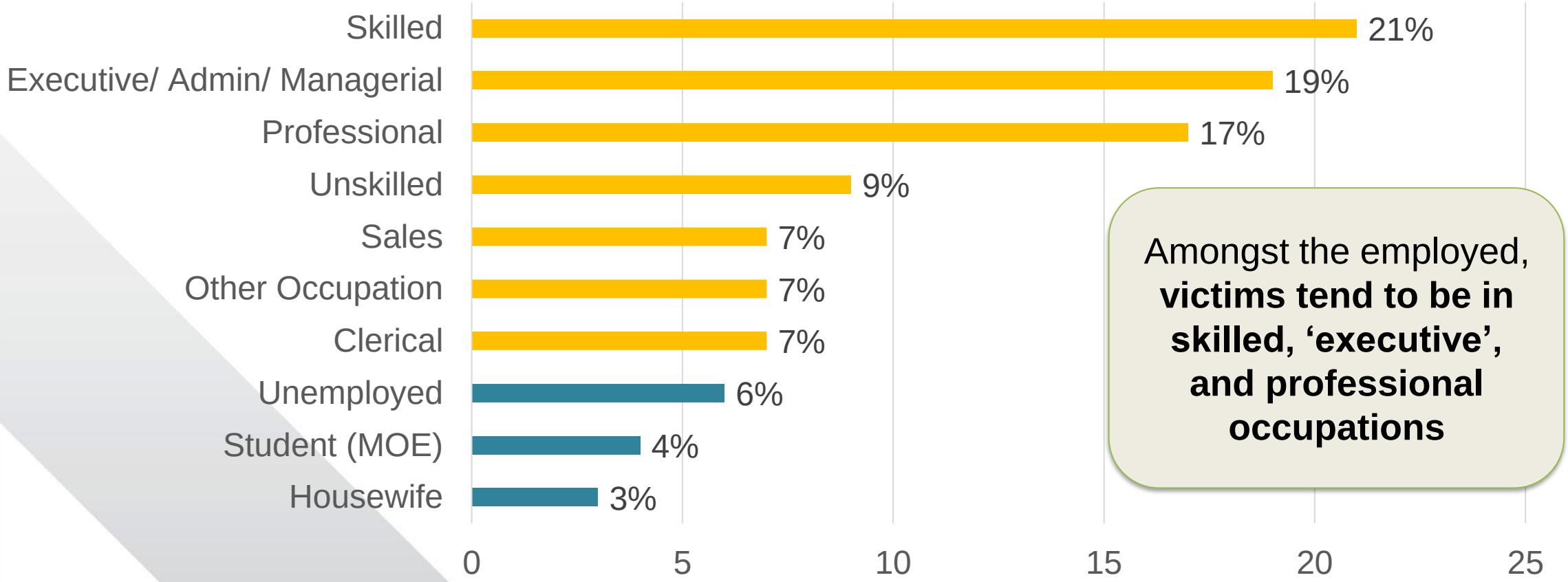


87% of victims are gainfully employed

Pre-Conversation | First Monetary Transfer | Sub. Monetary Transfer | Realisation

General Demographic Information

Occupation of Victims (*N*=270)



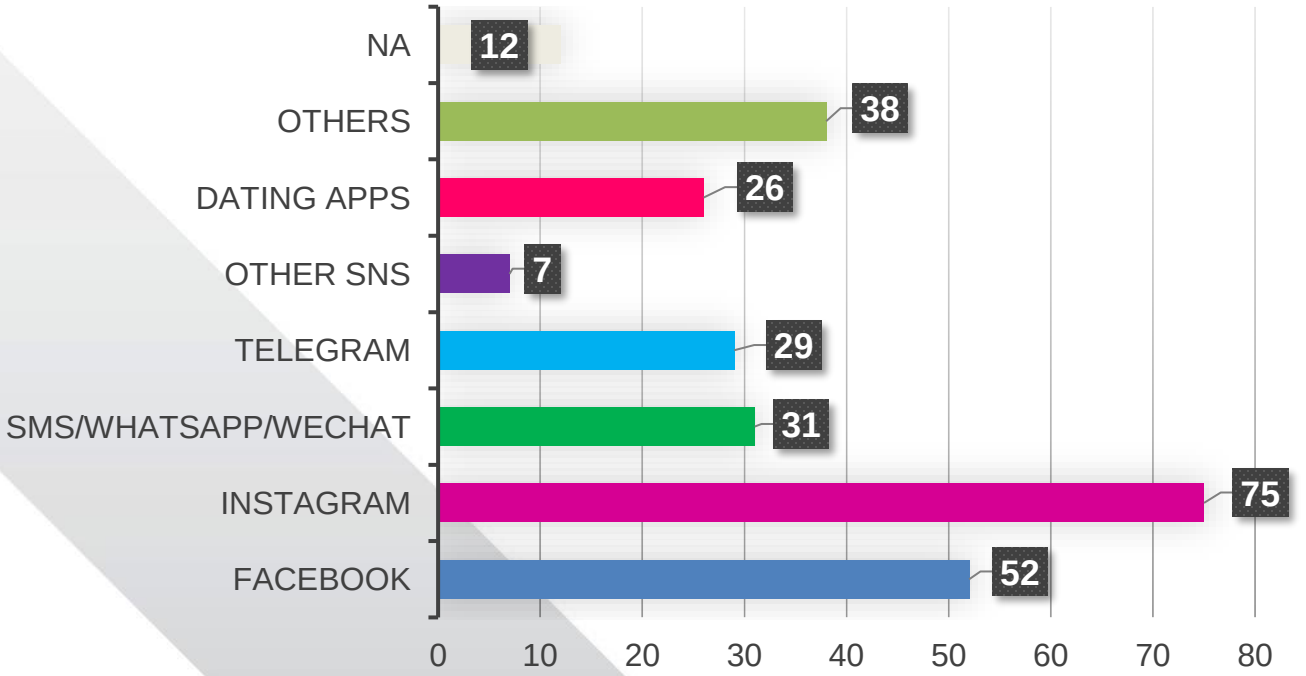
Amongst the employed, **victims tend to be in skilled, 'executive', and professional occupations**

Pre-Conversation | **First Monetary Transfer** | **Sub. Monetary Transfer** | **Realisation**

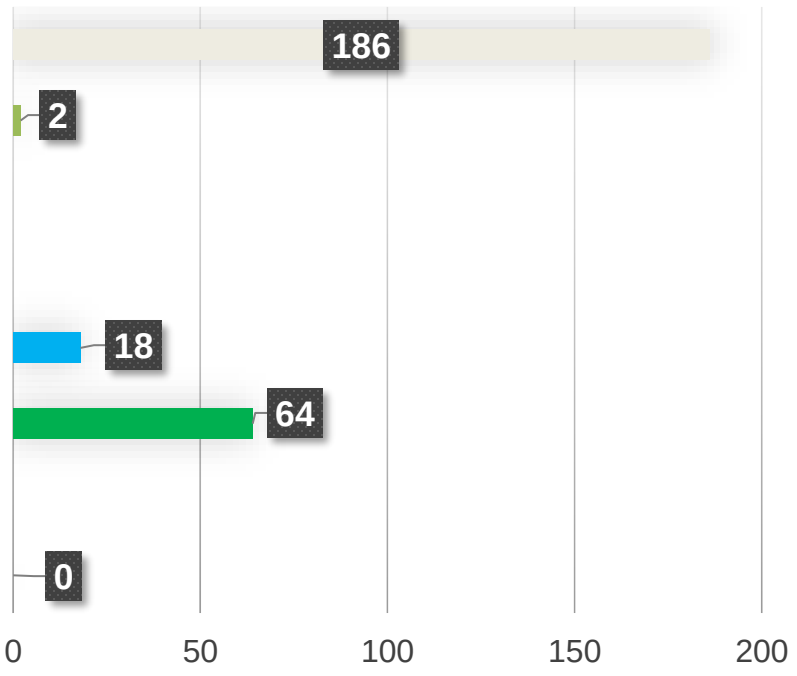
Platform of Contact used in Investment Scams

- Significant difference found between Initial and Subsequent Platform of Contact, X^2 (21, N = 270) = 45.36, p = .002 (sig)

Initial Point of Contact (*N*=270)



Subsequent Point of Contact (*N=270*)

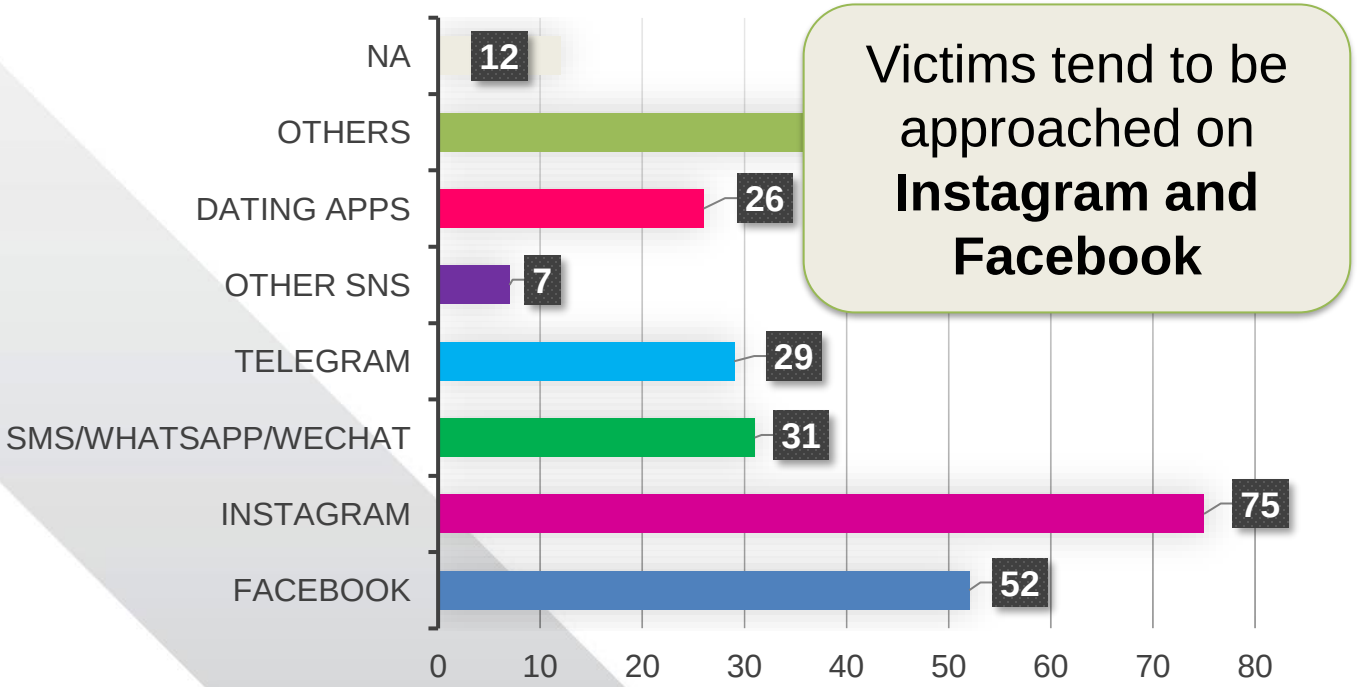


Pre-Conversation (contact) | **First Monetary Transfer** | **Sub. Monetary Transfer** | **Realisation**

Platform of Contact used in Investment Scams

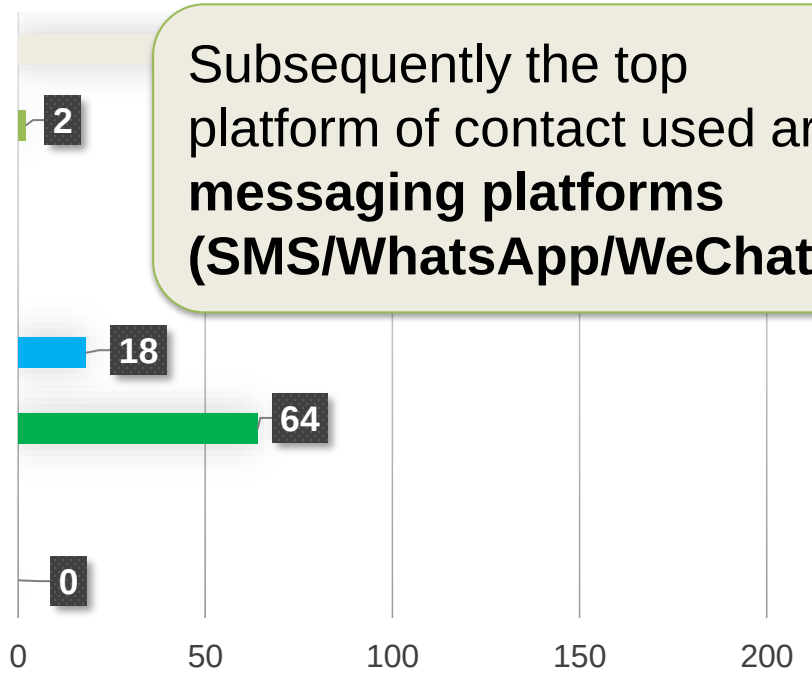
- Significant difference found between Initial and Subsequent Platform of Contact, X^2 (21, N = 270) = 45.36, p = .002 (sig)

Initial Point of Contact (*N*=270)



Victims tend to be approached on **Instagram and Facebook**

Subsequent Point of Contact (*N=270*)

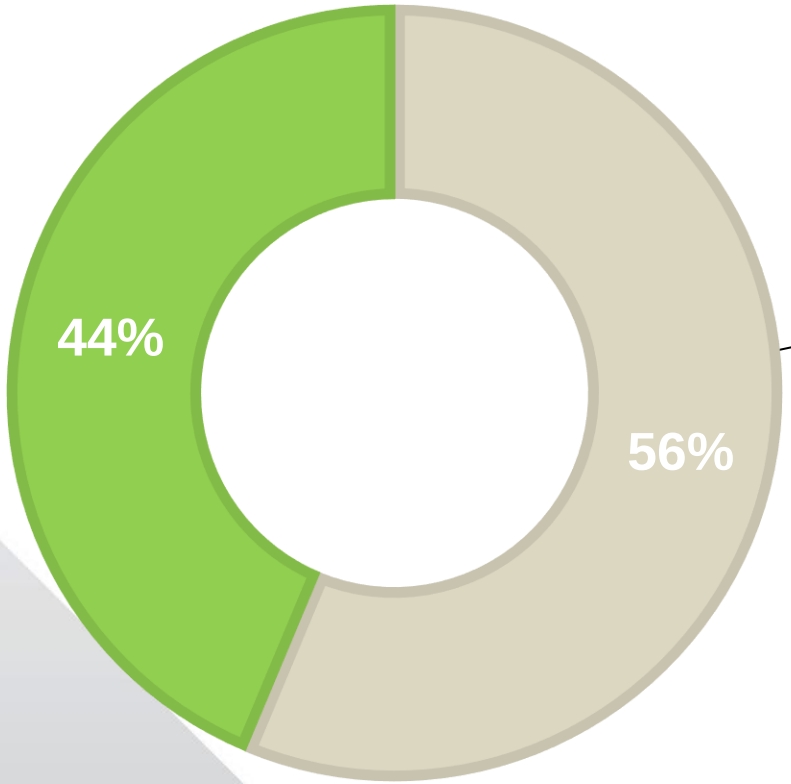


Subsequently the top platform of contact used are **messaging platforms (SMS/WhatsApp/WeChat)**

Pre-Conversation | **First Monetary Transfer** | **Sub. Monetary Transfer** | **Realisation**

Tools employed in Investment Scams

- Presence of Customer Service (*N*=270)



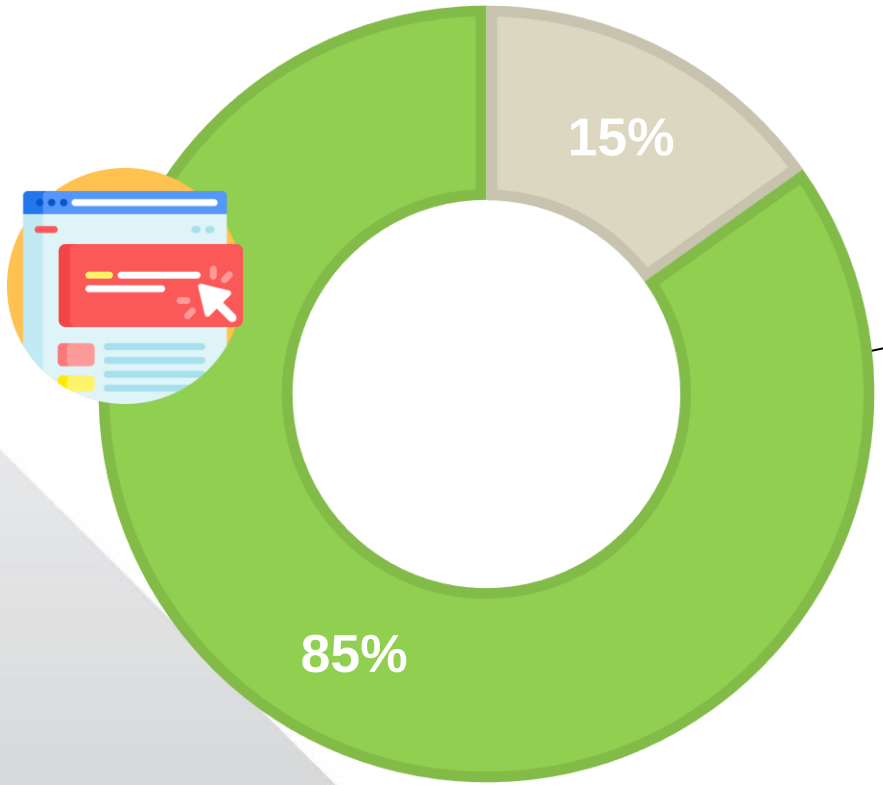
44% of victims experienced customer service during the investment scam

- ***Third party that helps with top-ups, queries, provides "investment" guidance***

Pre-Conversation | **First Monetary Transfer** | **Sub. Monetary Transfer** | **Realisation**

Tools employed in Investment Scams

- Presence of Website/Application (*N*=270)

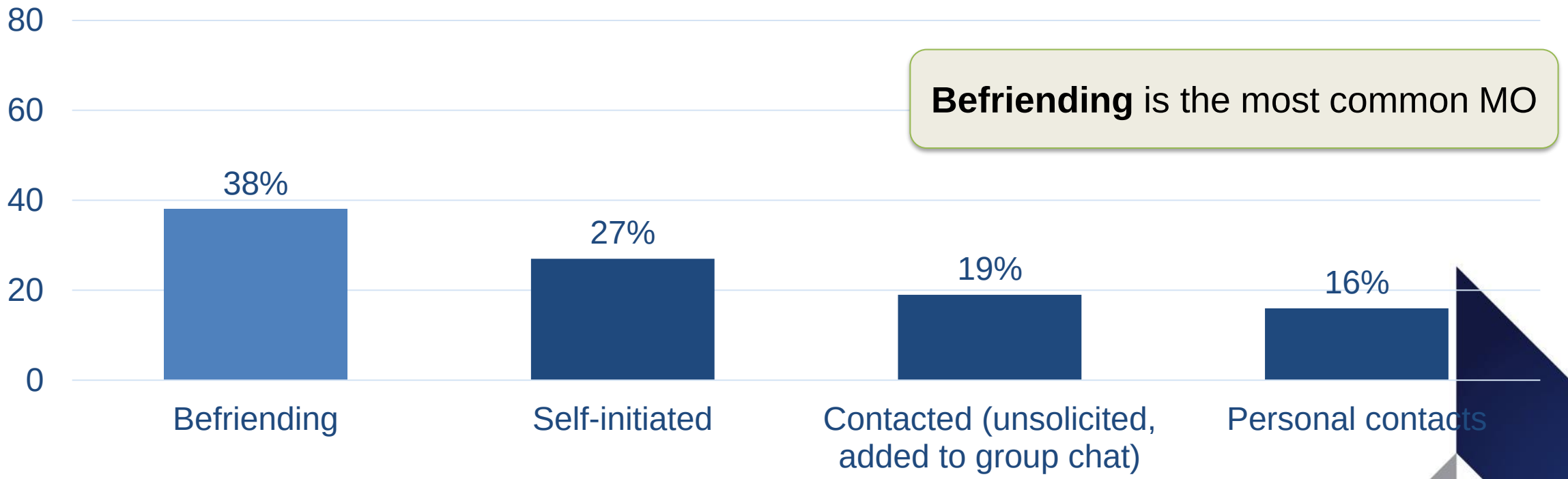


85% of victims encountered a (spoofed) website or application during the investment scam

Pre-Conversation | **First Monetary Transfer** | **Sub. Monetary Transfer** | **Realisation**

Modus Operandi (MO): Dimensions & Definitions

- The classification of MO follows PID's classification of investment scams (i.e. befriending, added to group chat, self-initiated), with the addition of unsolicited contact from scammers and introduction via personal contacts
- *N*=234 (N=36 excluded due to insufficient information)



Befriending is the most common MO

Pre-Conversation | **First Monetary Transfer** | **Sub. Monetary Transfer** | **Realisation**

MO: Dimensions and Definitions

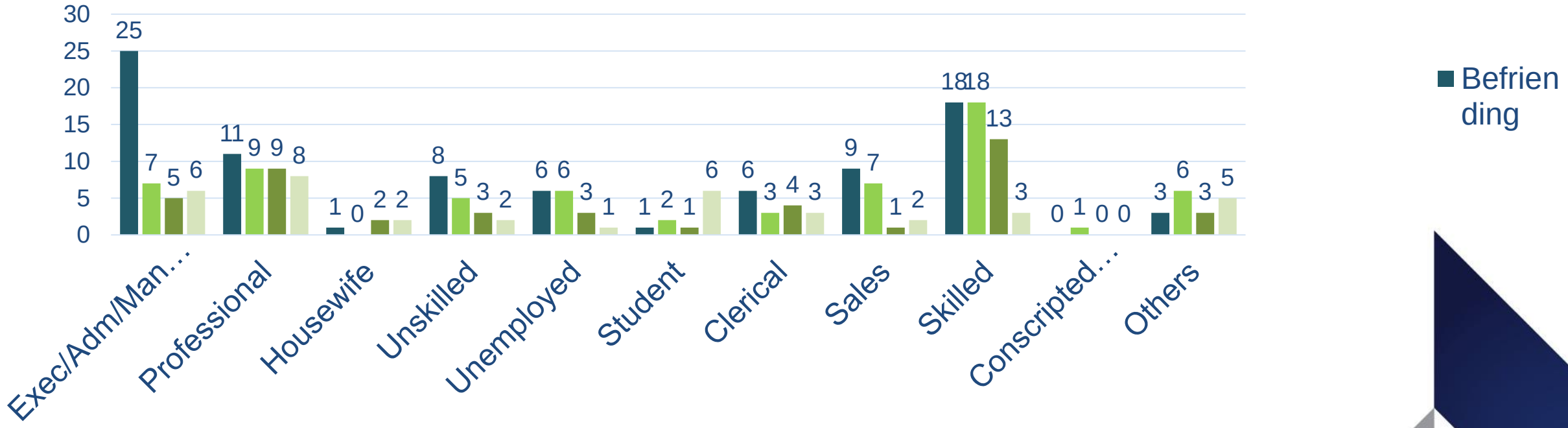
Dimension	Definition	*N*
Befriending	Scammers build a relationship (platonic or romantic) with the potential victim. Involve a period of frequent conversation and fostered camaraderie/ attraction before providing “investment opportunity”.	**88**
Self-initiated	Victim responded to outreach or online advertisement.	**64**
Contacted (unsolicited, added to group chat)	Victim added to a group chat or contacted by scammer with an unsolicited investment opportunity.	**44**
Personal contacts	Victim responded to personal contact’s online advertisement of “investment opportunity” or was contacted by personal contact with an “investment opportunity”.	**38**

Does MO significantly differ amongst victims of different demographics?

Overview of Results:		
Variable	**Analysis**	**Results**
Gender	Chi-square	Non-significant
Citizenship		
Occupation		**Significant**

Relationship between MO and Occupation

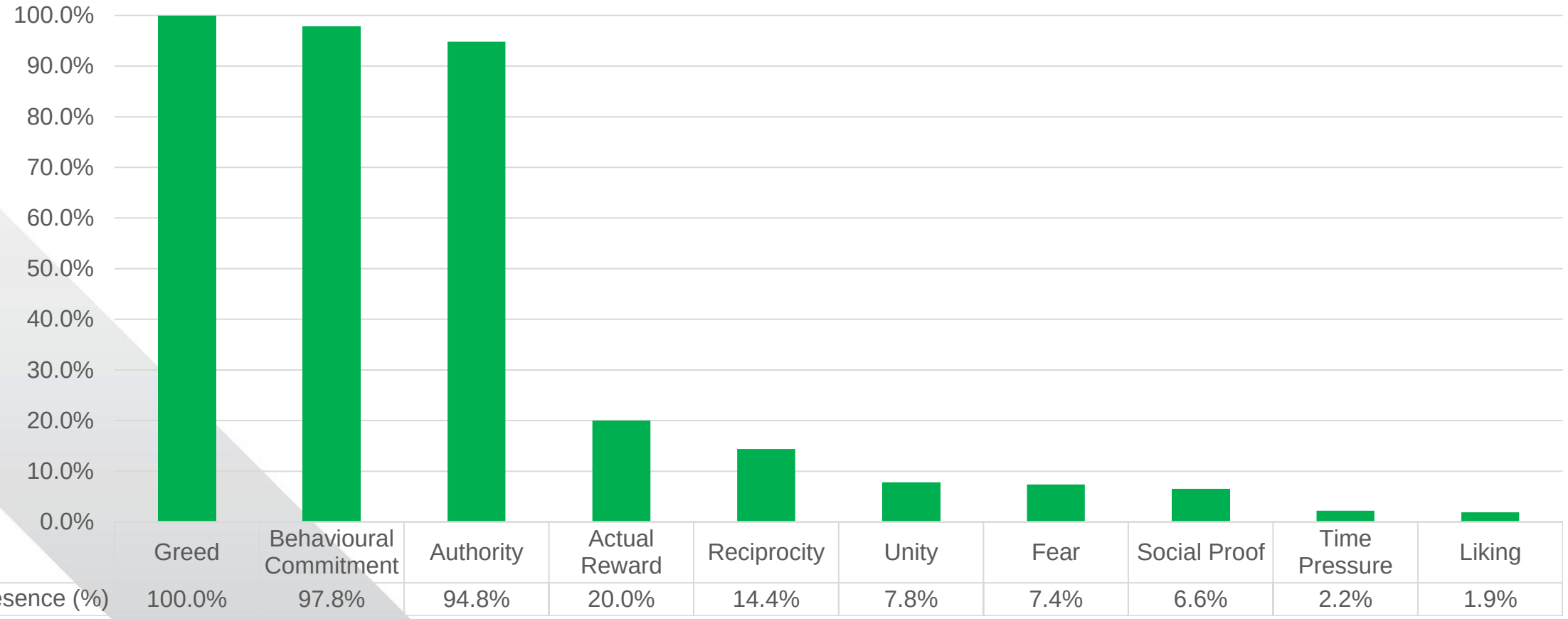
- Significant relationship found between MO and occupation, X^2 (30, N = 234) = 47.89, p = .020 (sig)
- *N*=234 (N=36 excluded due to insufficient information)



Pre-Conversation | First Monetary Transfer | Sub. Monetary Transfer | Realisation

Presence of Psychological Principles

N = 270



	Greed	Behavioural Commitment	Authority	Actual Reward	Reciprocity	Unity	Fear	Social Proof	Time Pressure	Liking
Presence (%)	100.0%	97.8%	94.8%	20.0%	14.4%	7.8%	7.4%	6.6%	2.2%	1.9%

Pre-Conversation | First Monetary Transfer | Sub. Monetary Transfer | Realisation

Presence of Psychological Principles

Dimension	Definition	%
Greed (Visceral cue)	Presence of visceral cues and triggers that appeal to basic human desires (Greed) to lure and motivate the victim into compliance. ***E.g. Paywall (to unlock higher tiered rewards), or other narratives that evoke greed such as rags-to-riches tropes (easy and high rewards).***	**100**
Behavioural Commitment	Small steps that subject victims to higher susceptibility of falling prey to future larger request by leveraging on the innate need for consistency. ***E.g. Acts like creating an account, completing multiple tasks.***	**97.8**
Authority	Impersonation of authority figures or legitimate companies/ organisations to elicit trust in victims, leveraging on the tendency of compliance to authority. ***E.g. Claiming to be from a legitimate company, providing official-looking documents (proof of business), provides spoofed websites/ applications/ logos.***	**94.8**

Presence of Psychological Principles

Dimension	Definition	%
Actual Reward (Bait)	Promised incentives that are received by the victim that legitimises the process. ***E.g. Receiving a monetary transfer back after the initial monetary transfer.***	20
Reciprocity	Altruistic actions and gifts of goodwill that leverage on the tendency to return favours. ***E.g. 'Friend' offer to help victim pay for the required funds or offer trial credits.***	14.4
Unity	Fostering an in-group identity within the victim. ***E.g. Invited into chatgroups with others doing the same 'job'.***	7.8
Fear (Visceral cue)	Presence of visceral cues that evoke the feeling of fear, often associated with sunk cost. ***E.g. Threatening victims with legal action or revenge if they do not comply.***	7.4

Presence of Psychological Principles

Dimension	Definition	%
Social Proof	Presence of trust-inducing cues from social environment to reinforce request. ***E.g. Receiving screenshots, as proof of receiving the investment payout, by others in chatgroups to reinforce legitimacy of offer/ earnings.***	6.6
Scarcity	Presence of urgency and scarcity cues that lowers ability for rational decision making ***E.g. "Within 24 hours", "Limited to", "Urgent"***	2.2
Liking	Fostering a positive impression or winning the victims' adoration and trust. Leverage on the inclination to sources that are well-liked. ***E.g. Grooming behaviours (frequent texting/ romantic interest) or using an attractive profile picture.***	1.9

Do Psychological Principles differ amongst MO?

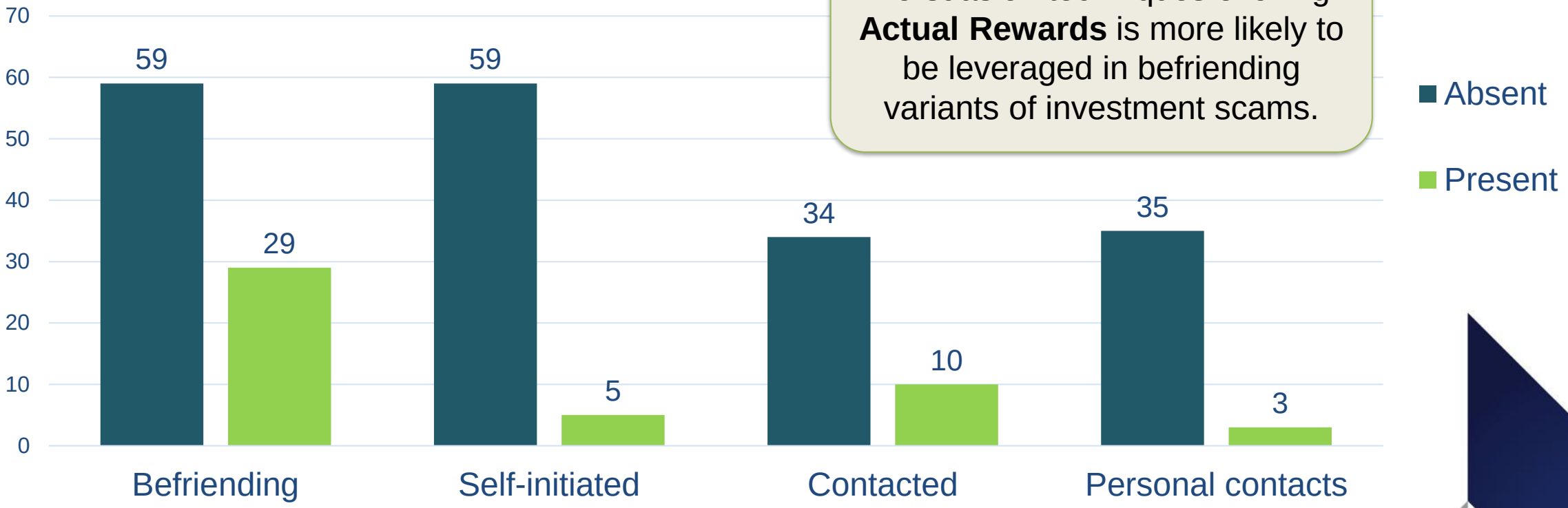
Overview of Results:		
Variable	**Analysis**	**Results**
Greed is present for ALL cases		
Time pressure	Chi-Square	Non-significant
Social proof		
Authority		
Behavioural Commitment		
Fear		
Assurance		
Actual rewards		**Significant**
Unity		
Reciprocity		
Liking		

Pre-Conversation | First Monetary Transfer | Sub. Monetary Transfer | Realisation

Relationship between Actual Rewards and MO

- Significant relationship found between Actual Rewards and MO for investment scams, X^2 (3, N = 234) = 18.80, p = .000 (sig)

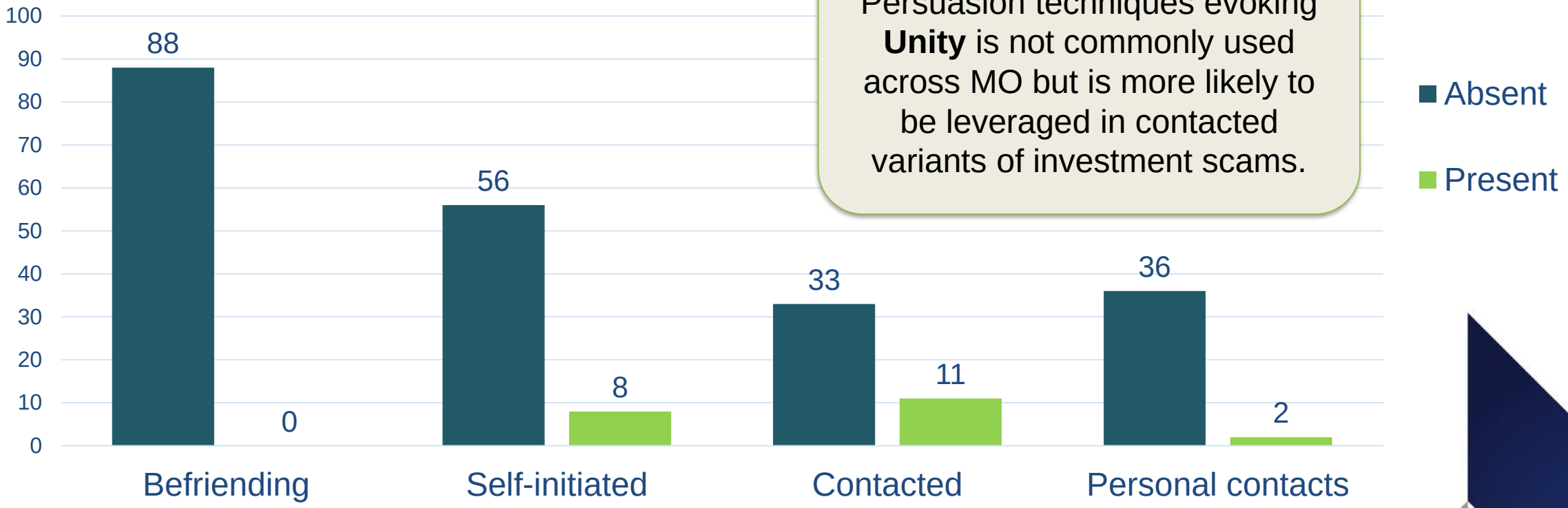
Persuasion techniques evoking **Actual Rewards** is more likely to be leveraged in befriending variants of investment scams.



Pre-Conversation | First Monetary Transfer | Sub. Monetary Transfer | Realisation

Relationship between Unity and MO

- Significant relationship found between Unity and MO for investment scams, X^2 (3, N = 234) = 24.12, p = .000 (sig)



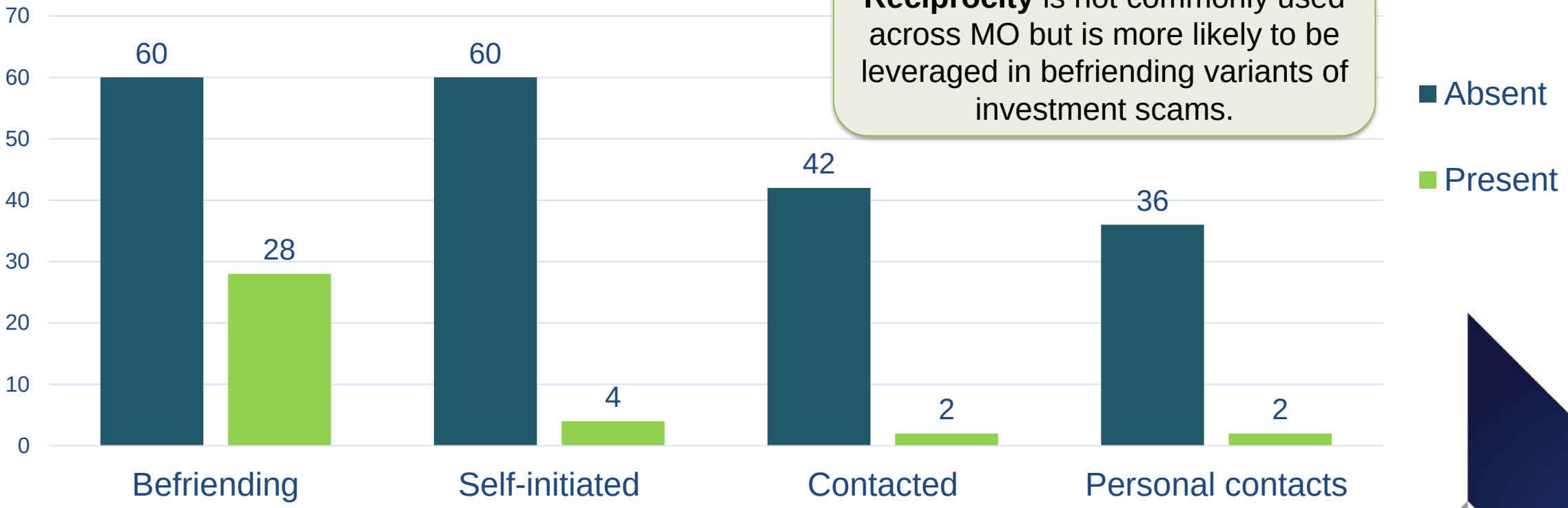
Persuasion techniques evoking **Unity** is not commonly used across MO but is more likely to be leveraged in contacted variants of investment scams.

Pre-Conversation | First Monetary Transfer | Sub. Monetary Transfer | Realisation

Relationship between Reciprocity and MO

- Significant relationship found between Reciprocity and MO for investment scams, X^2 (3, N = 234) = 29.32, p = .000 (sig)

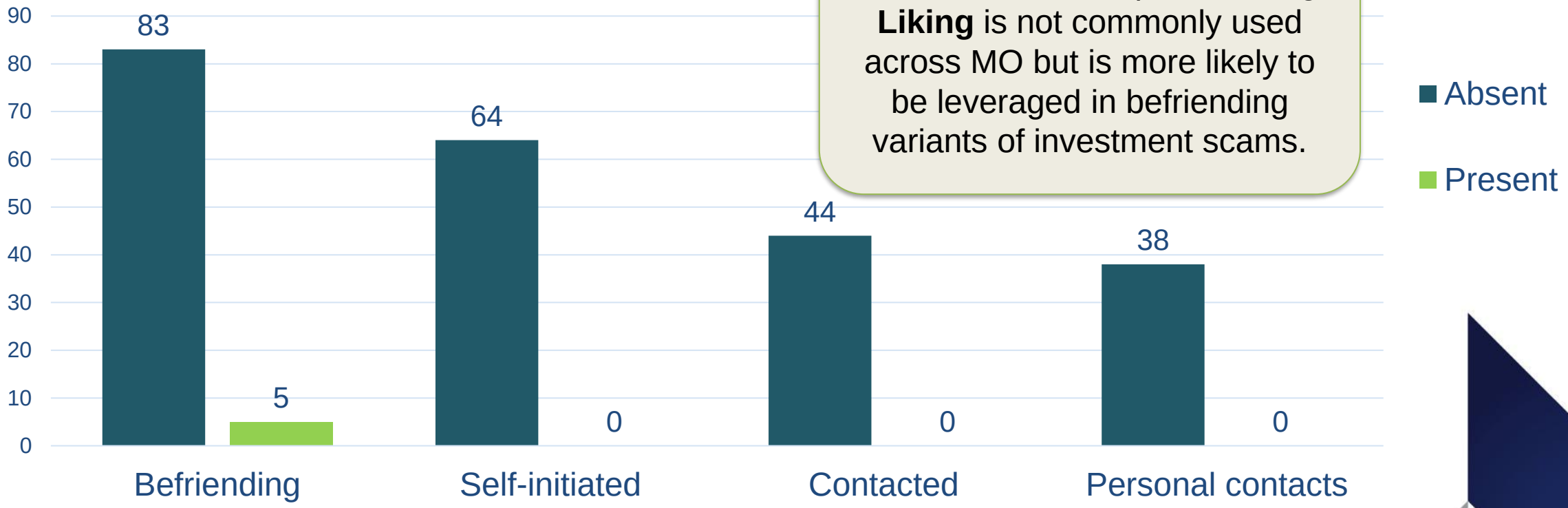
Persuasion techniques evoking **Reciprocity** is not commonly used across MO but is more likely to be leveraged in befriending variants of investment scams.



Pre-Conversation | First Monetary Transfer | Sub. Monetary Transfer | Realisation

Relationship between Liking and MO

- Significant relationship found between Liking and MO for investment scams, X^2 (3, N = 234) = 8.48, p = .037 (sig)



Persuasion techniques evoking **Liking** is not commonly used across MO but is more likely to be leveraged in befriending variants of investment scams.

Pre-Conversation | First Monetary Transfer | Sub. Monetary Transfer | Realisation

Do Psychological Principles differ between Gender?

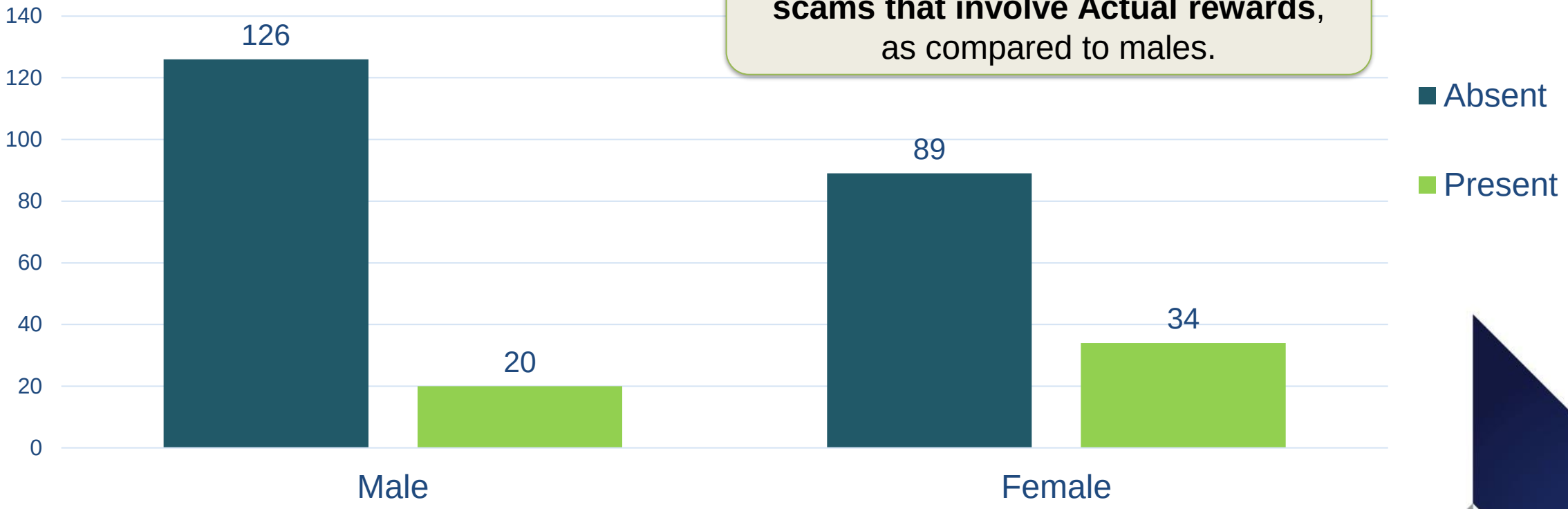
Overview of Results:		
Variable	**Analysis**	**Results**
Greed is present for ALL cases		
Time pressure	Chi-Square	Non-significant
Unity		
Social proof		
Authority		
Behavioural Commitment		
Fear		
Liking		
Actual rewards		**Significant**
Reciprocity		

Pre-Conversation | First Monetary Transfer | Sub. Monetary Transfer | Realisation

Relationship between Actual rewards and Gender

- Significant relationship found between Actual rewards and Gender for Investment scams, X^2 (1, N = 269) = 8.09, p = .004 (sig)

Females are more likely to fall for scams that involve Actual rewards, as compared to males.

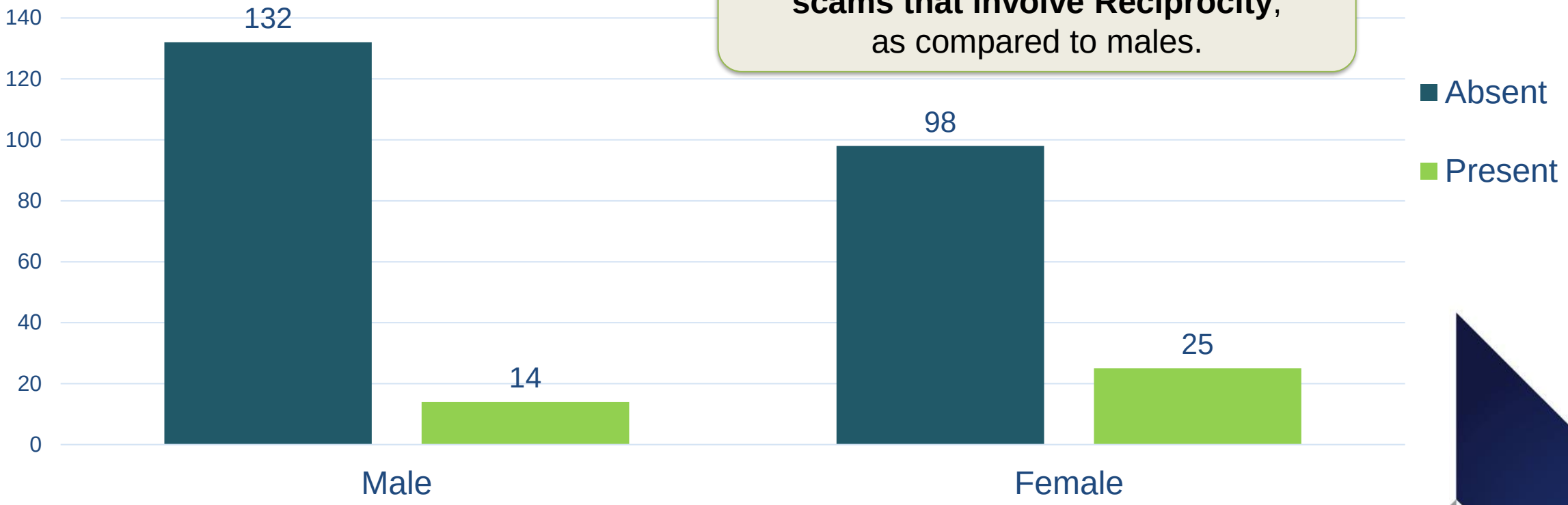


Pre-Conversation | First Monetary Transfer | Sub. Monetary Transfer | Realisation

Relationship between Reciprocity and Gender

- Significant relationship found between Reciprocity and Gender for Investment scams, X^2 (1, N = 269) = 6.21, p = .013 (sig)

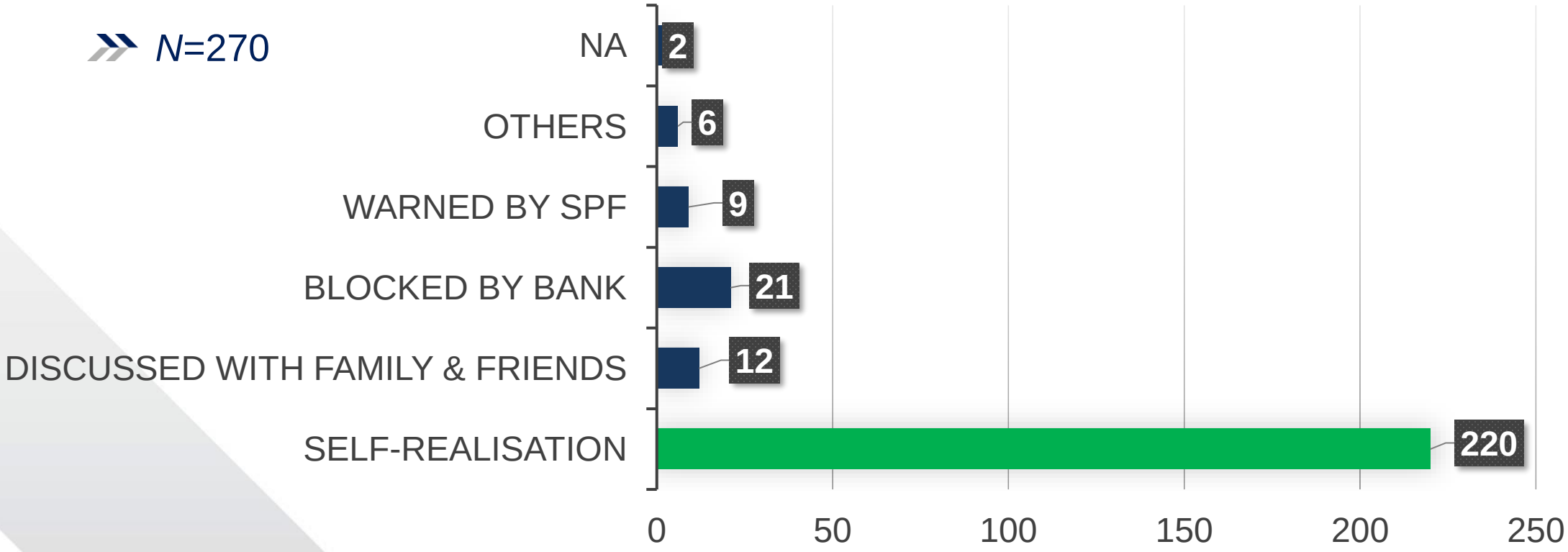
Females are more likely to fall for scams that involve Reciprocity, as compared to males.



Pre-Conversation | First Monetary Transfer | Sub. Monetary Transfer | Realisation

Reason for reporting

- *N*=270

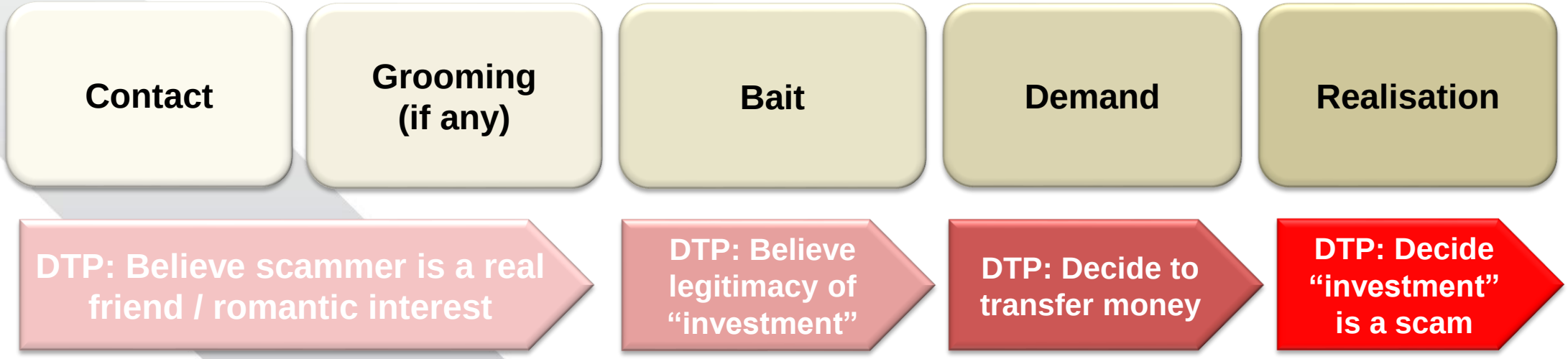


- Mode of realisation is not significantly affected by MO

6. Crime Prevention

Process of Investment Scam

- Scam prevention messages should help the public make better decisions at key Decision Tipping Points (DTP) as identified below
- 3 categories of scam prevention messages: red flags, scam process related, call to action



Investment Scam Crime Prevention

Findings	DTP Targeted	Scam Prevention Message
Top 2 platforms of subsequent contact with victims: • SMS/WhatsApp/WeChat (24%) • Telegram (7%)	**DTP: Believe scammer is a real friend / romantic interest** Knowledge of red flags during initial stage of scam helps introduce perception that the person they are interacting with might be a scammer	**Red flag:** Realise that movement from social media platforms to messaging platforms is likely to happen in investment scams

Investment Scam Crime Prevention

Findings	DTP Targeted	Scam Prevention Message
Victims reported having experienced grooming – a social influence strategy used by scammers to gain trust, resulting in shallow-information processing and subsequent decision errors.	**DTP: Believe scammer is a real friend / romantic interest** • Message should challenge victim's perception that the relationship is legitimate • As victim progresses deeper into the scam, chances of cognitive vulnerabilities being exploited increase • More effective if victim can identify scams and stop themselves at earlier DTPs	**Scam process related** Mention that everyone can be a victim as scammers prey on human needs (i.e. companionship, loneliness). Reduces psychological distance as message becomes more relatable. **Call to action** Mention ways public can verify legitimacy of the relationship (i.e. video call / meet up, not voice recording as that can be altered)

Crime Prevention Concept

DTP: Believe scammer is a real friend / romantic interest

- Quotes from victims on how grooming affects decision-making

Loneliness increases vulnerability to scammers

"So I would say in terms of loneliness, that is that portion of it. Now to think of it, I think that was one of the main thing that maybe made me fall for this whole thing"

Lack of awareness on how everyone is vulnerable to scams due to grooming

"Yes, I have [seen posters], but I never would have thought that I myself would fall victim to one of these scams...They make you believe that they need you, take such good care of you…so that you won't think about the money."

When trust is built, increases victim's vulnerability to believing scammer

"And so I think this person, they're very well-trained and professional about it in that sense. The conversations that we have right, and the trust that was built on for me towards him was really, you know, something very solid that even if I hear, I see, I may not, I may still, I may not, believe that he's a fake, in that sense, or he's a scammer."

"So I was thinking…why not try? I mean, it's in the back of my mind… because the lady already talked to me every single day for one and a half months. It sounded so innocent."

Investment Scam Crime Prevention

Findings	DTP Targeted	Scam Prevention Message
Victims reported receiving actual monetary rewards after the initial few transfers.	**DTP: Believe legitimacy of "investment"** • Scammers leverage on legitimacy by giving actual rewards • Messages should help victims make a better decision on legitimacy	**Call to action** Messages state ways public can verify legitimacy of investment: • Should not be transferring to personal numbers via PayNow + multiple numbers with different name • Verification should be done externally with trusted persons, not with the same source (i.e. when scammers give actual rewards, other "investors" earning profits) • Check legitimacy of company by verifying with registry of companies

Scam Prevention Concept

DTP: Believe legitimacy of "investment"

- Quotes from victims on how actual rewards and words from other "investors" lead them into erroneously believing in legitimacy of "investment"

Victims believed "investment" was legitimate as they received actual rewards (initially)

"that time I was also very cautious that, you know, I put in, am I able to take out and stuff like that. So yes, I was able to take out initially…because I was able to take out, so I thought, actually quite okay"

"And so I deposit $500 I think…I end up making…at least 80% of money back or 50% of my money back but after two nights or something like that…then she was asking me, do you have any more money to invest because you can get better returns. So I thought you know, maybe this is real…just onto a good thing."

Victim believed "investment" was legitimate due to other "investors" in group chat

"They are posting wow these people make money, DBS receipt show how much they put in and how much the person got back. So it sounds very convincing, the receipt looks so real, doesn't look like a fake receipt and so many people post like that."

Investment Scam Prevention

Findings	DTP Targeted	Scam Prevention Message
Victims experienced behavioural commitment – small steps that subject victims to higher susceptibility of falling prey to future larger request by leveraging on the innate need for consistency.	**DTP: Decide to make first and subsequent transfers** • Message should challenge decision to make the first transfer and subsequent transfers	**Scam process related** • Inform public that trying out with a small amount is more dangerous than they think as it is difficult to stop after the first transfer **Call to action** • Inform public to involve trusted persons before making a transfer – a more direct intervention might be needed during subsequent transfers, where emotions and cognitive biases are at play to a larger extent

Scam Prevention Concept

DTP: Decide to make first and subsequent transfers

- Quotes from victim on reasons for making first transfer and the difficulty of stopping thereafter

Victim made first transfer as it was perceived as small and harmless

"because the first was not that big amount of money since I saw the returns right that's okay, then I would try with that small amount of money, I'm still okay with that"

"Then he guaranteed me and said, if let's say, you know, if it's a scam, the most you lose is this initial amount of $1,000 that you put. It's something because at the end of the day, no investment is risk-free, etc."

Sunk cost fallacy driving victim to continue transferring money

"Because in my mind I'm thinking that, okay, no choice already, already put so much. So, continue the game."

"there was really a point of time where I almost gave in and then transfer whatever I had left…it was how they tackled the desperation you know so that you want to top up to try to get the rest of it out."

Implication on Investment Scam Prevention

Data	DTP Targeted	Scam Prevention Message
Victims realise they have been scammed when they are unable to withdraw money.	**DTP: Decide "investment" is a scam** • Message should help victims to bring forward the realisation that they are being scammed	**Call to action** • Encourage victims to request for withdrawal earlier, before making multiple transfers

Scam Prevention Concept

DTP: Decide "investment" is a scam

- Quotes from victims on realisation of scam

Victims realised they are scammed when they are unable to withdraw money despite complying with multiple requests

"So this time round, same thing, the person promised next day I will have double my return or what, and I can withdraw, how come I cannot withdraw? So this is a bit, not proper already, so the red flag is stuck already."

"Then when that thing happened, then after that, the moment I realised the whole thing was kind of screwed up was, you realised that you cannot withdraw the money. They rejected the withdrawal of the money. Then that's why I was like, oh, it's something that I didn't anticipate that you cannot withdraw the money. Then that's how everybody also realised that it's like a scam."

7. Limitations

Limitations

- Lack of data fields in statement of facts to perform more in-depth analysis for psychological processes
- Smaller sample size of victims for in-depth interviews; victims unwilling to be interviewed

SINGAPORE POLICE FORCE
SAFEGUARDING EVERY DAY

Thank you

Email Carolyn_MISIR@spf.gov.sg