



NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

**LAUNDERING LOVE: A MULTI-CASE ANALYSIS
OF THE EVOLUTION OF ROMANCE SCAM VICTIMS
INTO CO-OFFENDING MONEY MULES**

by

Christopher K. Huhn

March 2023

Co-Advisors:

Christopher Bellavita (contractor)
Kathryn J. Aten

Approved for public release. Distribution is unlimited.

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			<i>Form Approved OMB No. 0704-0188</i>	
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington, DC, 20503.				
1. AGENCY USE ONLY (Leave blank)		2. REPORT DATE March 2023	3. REPORT TYPE AND DATES COVERED Master's thesis	
4. TITLE AND SUBTITLE LAUNDERING LOVE: A MULTI-CASE ANALYSIS OF THE EVOLUTION OF ROMANCE SCAM VICTIMS INTO CO-OFFENDING MONEY MULES			5. FUNDING NUMBERS	
6. AUTHOR(S) Christopher K. Huhn				
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000			8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A			10. SPONSORING / MONITORING AGENCY REPORT NUMBER	
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.				
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release. Distribution is unlimited.			12b. DISTRIBUTION CODE A	
13. ABSTRACT (maximum 200 words) This thesis addresses the problems of rapidly rising cyber-enabled fraud and concomitant money laundering by focusing on romance scam victims who evolve into willing partners in money laundering schemes, known as "witting money mules." This thesis explores how and why individuals become money mules after victimization in online romance scams. The thesis employs a grounded theory approach and investigates data from over 134,000 historical text messages between three offenders and 22 victims, as well as three participant interviews with romance scam victims. The data resulted in a grounded theory that a romantically lonely victim who persistently engages online with an offender that strategically repeats scheme-relevant premises in the guise of a romantic partner can result in the victim acceding to the offender's exploitative requests and the eventual decision to co-offend. This theory also explains how a person can simultaneously be a victim and offender and why they would intentionally choose to help the romance scammer launder money. The literature and data similarly support a suggested definition for "grooming" in the context of romance scams. As a whole, this thesis provides insight into romance scams and money mules as a strategic pivot point that, if disrupted, can simultaneously impact a criminal organization's ability to profit from romance scams and launder the proceeds of cyber-enabled fraud.				
14. SUBJECT TERMS romance scam, sweetheart scam, romance fraud, confidence fraud, money laundering, money mule, transnational criminal organizations, grooming, cyber-enabled fraud, cybercrime, catfishing, co-offending, repetition-induced truth, referential theory, grounded theory			15. NUMBER OF PAGES 181	
			16. PRICE CODE	
17. SECURITY CLASSIFICATION OF REPORT Unclassified	18. SECURITY CLASSIFICATION OF THIS PAGE Unclassified	19. SECURITY CLASSIFICATION OF ABSTRACT Unclassified	20. LIMITATION OF ABSTRACT UU	

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. Z39-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release. Distribution is unlimited.

**LAUNDERING LOVE: A MULTI-CASE ANALYSIS OF THE EVOLUTION OF
ROMANCE SCAM VICTIMS INTO CO-OFFENDING MONEY MULES**

Christopher K. Huhn
Supervisory Special Agent, Minnesota Commerce Fraud Bureau
BS, Mankato State University, 1996

Submitted in partial fulfillment of the
requirements for the degree of

**MASTER OF ARTS IN SECURITY STUDIES
(HOMELAND SECURITY AND DEFENSE)**

from the

**NAVAL POSTGRADUATE SCHOOL
March 2023**

Approved by: Christopher Bellavita
Co-Advisor

Kathryn J. Aten
Co-Advisor

Erik J. Dahl
Associate Professor, Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

This thesis addresses the problems of rapidly rising cyber-enabled fraud and concomitant money laundering by focusing on romance scam victims who evolve into willing partners in money laundering schemes, known as “witting money mules.” This thesis explores how and why individuals become money mules after victimization in online romance scams. The thesis employs a grounded theory approach and investigates data from over 134,000 historical text messages between three offenders and 22 victims, as well as three participant interviews with romance scam victims. The data resulted in a grounded theory that a romantically lonely victim who persistently engages online with an offender that strategically repeats scheme-relevant premises in the guise of a romantic partner can result in the victim acceding to the offender’s exploitative requests and the eventual decision to co-offend. This theory also explains how a person can simultaneously be a victim and offender and why they would intentionally choose to help the romance scammer launder money. The literature and data similarly support a suggested definition for “grooming” in the context of romance scams. As a whole, this thesis provides insight into romance scams and money mules as a strategic pivot point that, if disrupted, can simultaneously impact a criminal organization’s ability to profit from romance scams and launder the proceeds of cyber-enabled fraud.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

I.	INTRODUCTION.....	1
A.	PROBLEM STATEMENT	1
B.	RESEARCH QUESTIONS.....	3
C.	ROMANCE SCAM LITERATURE REVIEW.....	4
1.	Victim-Centered Romance Scam Studies	5
2.	Subject-Centered Romance Scam Studies.....	11
3.	Prevention-Centered Romance Scam Studies	11
D.	OVERVIEW OF MONEY LAUNDERING.....	13
1.	The Money Laundering Cycle	13
2.	The Bank Secrecy Act and USA PATRIOT Act.....	14
3.	Money Laundering and the BSA	15
4.	Money Mules	17
E.	CONTRIBUTION.....	20
II.	METHODS	23
A.	FIELD INTERVIEW CASES.....	26
1.	Recruitment Efforts	26
2.	Field Interview Participants.....	27
3.	Data Collection	28
4.	Data Preparation.....	29
B.	ARCHIVAL CASES.....	29
1.	Data Preparation.....	30
2.	Initial Case Inclusion and Coding	31
3.	Thematic Sampling	32
C.	COMPARING INTERVIEWS AND ARCHIVAL CASES.....	33
III.	ANALYSIS OF OFFENDER COMMUNICATION.....	37
A.	GROOMING THE VICTIM	37
1.	Establishing a Persona.....	38
2.	Developing and Maintaining a Relationship	42
3.	Inducing Gullibility.....	47
B.	EXPLOITING THE VICTIM OR MONEY MULE.....	55
1.	Swindling	55
2.	Money Laundering.....	59
3.	Problem-solving.....	63
C.	SUMMARY	66

IV.	VICTIM AND MONEY MULE COMMUNICATIONS	69
A.	ENGAGING THE PERSONA.....	69
1.	Emotional Loneliness.....	70
2.	Developing and Maintaining a Relationship	73
3.	Assessing Credibility.....	78
B.	ASSISTING THE PERSONA.....	87
1.	Helping a Loved One	87
2.	Acting as a Money Mule	92
3.	Problem-Solving.....	95
C.	SUMMARY	99
V.	THE PATH THROUGH ROMANCE SCAMS TO CO-OFFENDING.....	101
A.	HOW DO INDIVIDUALS BECOME MONEY MULES AFTER BEING VICTIMIZED IN ONLINE ROMANCE SCAMS?	104
B.	WHY DO ALL ONLINE ROMANCE SCAM VICTIMS NOT ACT AS MONEY MULES?	108
C.	DISCUSSION AND FUTURE RESEARCH QUESTIONS	109
1.	Victim Susceptibility	110
2.	The Role of Attraction, Vividness, and Repetition in Belief Formation.....	111
3.	Proposed Definition of Grooming.....	115
4.	Co-offending	117
5.	A Grounded Theory of the Evolution of Individuals into Co-offending Money Mules Through Engagement with Online Romance Scam Offenders.....	120
D.	LIMITATIONS.....	123
E.	RECOMMENDATIONS.....	123
1.	Romance Scam Warning Letter	124
2.	Persistent and Patient Engagement.....	124
3.	Technological Solutions.....	125
4.	Money Mule Investigations	125
F.	CONCLUSION	125
	APPENDIX A. STUDY DOCUMENTS	127
A.	EMAIL RECRUITMENT SCRIPT	127
B.	CONSENT FORM	128
C.	INTRODUCTORY SCRIPT.....	130
D.	INTERVIEW QUESTIONS	131
E.	POST-SCRIPT	135

APPENDIX B. ROMANCE SCAM SCRIPTS	137
APPENDIX C. ROMANCE SCAM WARNING LETTER.....	143
APPENDIX D. ADDITIONAL DATA TABLES.....	145
LIST OF REFERENCES	149
INITIAL DISTRIBUTION LIST	157

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

Figure 1.	Romance Scam Trajectories	7
Figure 2.	The Scammers Persuasive Techniques Model.....	9
Figure 3.	Data Structure	36
Figure 4.	The Path through Romance Scams to Co-offending.....	103

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

Table 1.	Select Bank Secrecy Act Report Types	15
Table 2.	Archival Cases	30
Table 3.	Date Range and Number of Texts per Identified Victim/Mule	33
Table 4.	Quotes Supporting Codes under the “Establishing a Persona” Theme	38
Table 5.	Quotes Supporting Code Formation under the “Developing and Maintaining a Relationship” Theme	42
Table 6.	Quotes Supporting Codes under the “Inducing Gullibility” Theme	48
Table 7.	Quotes Supporting Codes under the “Swindling” Theme	56
Table 8.	Quotes Supporting Codes under the “Money Laundering” Theme	60
Table 9.	Quotes Supporting Codes under the “Problem-solving” Theme	64
Table 10.	Quotes Supporting Codes under the “Emotional Loneliness” Theme	71
Table 11.	Quotes Supporting Codes under the “Developing and Maintaining a Relationship” Theme	73
Table 12.	Quotes Supporting Codes under the “Assessing Credibility” Theme	79
Table 13.	Quotes Supporting Codes under the “Helping a Loved One” Theme	88
Table 14.	Types and Frequencies of Sensitive Personal Identifiable Information Provided by Victims to Offenders	89
Table 15.	Quotes Supporting Codes under the “Acting as a Money Mule” Theme	93
Table 16.	Quotes Supporting Codes under the “Problem-solving” Theme	95
Table 17.	Presence of Codes in the “Grooming the Victim” Dimension	145
Table 18.	Presence of Codes in the “Exploiting the Victim or Money Mule” Dimension	146

Table 19.	Presence of Codes in the “Engaging the Persona” Dimension	146
Table 20.	Presence of Codes in the “Assisting the Persona” Dimension	147
Table 21.	Estimated Length of Money Mule Relationships	148

LIST OF ACRONYMS AND ABBREVIATIONS

8300	Report of Cash Payments Over \$10,000 in a Trade or Business
BEC	Business Email Compromise
BSA	Bank Secrecy Act
CHDS	Center for Homeland Defense and Security
CMIR	Currency and Monetary Instrument Report
CTR	Currency Transaction Report
DOJ	Department of Justice
FATF	Financial Action Task Force
FBI	Federal Bureau of Investigation
FFM	Five-Factor Model of Personality
FinCEN	Financial Crimes Enforcement Network
IC3	Internet Crime Complaint Center
Interpol	International Criminal Police Organization
IRB	Institutional Review Board
KYC	Know Your Customer
NPS	Naval Postgraduate School
PII	Personal Identifiable Information
RAT	Routine Activity Theory
SAR	Suspicious Activity Report

THIS PAGE INTENTIONALLY LEFT BLANK

EXECUTIVE SUMMARY

“Honey this our opportunity to be together mylove, i will never do anything that will hurt you, mylove noting bad is going to happen, i promise the money there is my money and its legit money and i trust you that is why you my beneficiary” (AS1 to AV1.1, August 2020).¹ This text message, taken from historical communications between an offender and victim in a romance scam, illustrates the type of narrative offenders use to justify transferring money through victims’ bank accounts. When victims participate, they act as “money mules” and help launder funds from other frauds. In this example, the offender represented funds stolen from the Payroll Protection Program as money owed to the offender’s persona from a purported manager. Thus, offenders exploit individuals via romance scams not only for their money, but for their help in laundering other fraud proceeds.

According to FBI reporting, romance scams result in significant financial harm to individuals, with losses approaching \$1 billion in 2021.² The fact that offenders groom money mules from among romance scam victims exacerbates the danger these scams pose. The intensification is due to money mules playing a significant role in laundering an additional \$6 billion in losses to other cybercrimes.³

This thesis focuses on money mules who were first victimized in romance scams because of the role this type of scam plays in generating financial victims and money laundering co-conspirators. Though scholarly and practitioner research mentions money mules, no study could be found that thoroughly explains the transformation from romance scam victim to co-conspirator. This thesis fills that theoretical gap by exploring how individuals become money mules after victimization in online romance scams and asking why they do not all act as money mules.

¹ This quote is provided as the offender wrote it, with grammatical and stylistic errors intact.

² Federal Bureau of Investigation, *Internet Crime Report 2021* (Washington, DC: Federal Bureau of Investigation, 2022), 7, https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf.

³ Federal Bureau of Investigation, 7.

A grounded theory approach was employed to analyze more than 134,000 historical text messages between three offenders and 22 victims to answer the research questions effectively. Three of these victims intentionally aided the offender with money laundering as money mules and accounted for 87% of the text messages. Three in-person interviews of romance scam victims augmented this historical data. Though none of the interviewees had acted as a money mule, their experiences helped develop more extensive insights into the grooming and exploitation processes. This data set allowed a unique look into romance scams and offenders' techniques to gain and maintain victim compliance.

A key finding of this research is the significant role repetition plays in the scam. The offender repeats scheme-relevant premises, which form the basis to justify exploitative requests, from the moment victimization begins, all the way through to co-offending. Previous research provides insight into why this strategy is effective. In the psychological literature, the concept that repetition affects an individual's judgment of truth is known as the repetition-induced truth effect.⁴ The literature explains that frequent exposure to a statement results in an individual's increasing belief that the statement is true.

Therefore, whether the offender frequently reaffirms love and commitment or repeats assertions of a large inheritance, each exposure creates stronger beliefs in the susceptible individual's mind. The offender then relies on these premises to make exploitative requests of the individual. Past romance scam research used the term *grooming* to refer to the offender's time spent preparing the victim to part with their money. In this thesis, *grooming* was found to be an offender's strategic manipulation of the repetition-induced truth effect. This study extended this new definition of grooming beyond romance scam victimization to co-offending as a money mule.

Another finding of this thesis is that a person can simultaneously be a romance scam victim and a co-offending money mule. That is, individuals can recognize that they are participating in a crime by transferring money, but still deny that the entire relationship is part of a scam. The psychological literature suggests that a commonly recognized error

⁴ Christian Unkelbach and Alex Koch, "Gullible but Functional? Information Repetition and the Formation of Beliefs," in *The Social Psychology of Gullibility: Fake News, Conspiracy Theories and Irrational Beliefs*, ed. Joseph P. Forgas and Roy F. Baumeister (New York, NY: Routledge, 2019), 43–44.

in decision-making related to the repetition-induced truth effect produces this phenomenon, rather than a victim characteristic.⁵

This study also demonstrates the utility of research by Free and Murphy on co-offending to explain a money mule's choice to offend. Free and Murphy find that "affective bonds" can be the basis for a person to choose to co-offend in fraud schemes.⁶ They find that intimate relationships can justify criminal conduct, even for those not generally inclined towards criminality. In the case of romance scams, individuals may deem illegal activity more desirable than the loneliness experienced before the relationship began.

Overall, this thesis makes several significant contributions toward understanding the money mule aspect of romance scams. First, it advances a grounded theory that a romantically lonely victim who persistently engages online with an offender that strategically repeats scheme-relevant premises in the guise of a romantic partner can result in the victim acceding to the offender's exploitative requests and an eventual decision to co-offend. Next, this study introduces a new definition of *grooming* and demonstrates the functionality of repetition-induced truth for understanding several observed phenomena. Additionally, it incorporates research on co-offending to explain money mule activity. Finally, a romance scam warning letter was developed to inform victims about the scam and warn them about acting as a money mule. Together, these developments are intended to aid researchers and practitioners in better understanding and, ideally, disrupting romance scams before the victim offends.

⁵ Unkelbach and Koch, 52.

⁶ Clinton Free and Pamela R. Murphy, "The Ties That Bind: The Decision to Co-Offend in Fraud," *Contemporary Accounting Research* 32, no. 1 (March 2015): 40–42, <https://doi.org/10.1111/1911-3846.12063>.

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

Our master's cohort developed a lot of sayings and slogans over the course of the 18-month program. Some are better suited than others to be quoted publicly. The most relevant slogan for an acknowledgments section went something like this: "Graduating is a team sport." I can say unequivocally I would not have made it through the program without a team.

First off, I would like to thank Angi English. After being out of college for 25 years, I was more than a little rusty at academic writing. You took the time to review my application essays and provide instructive feedback. With your help, I learned how to phrase my experience in academic terms. I would have not been admitted to the program without your assistance.

Then, of course, there are the members of Cohort 2105/2106. I thought it was rhetoric when the professors told us in the early days of the program that we would learn as much from each other as we would from them. It turned out to be very true for me. I appreciated the multiple perspectives everyone brought to our discussions and enjoyed watching different classmates become excited and engaged as we covered topics that particularly interested them. This journey would not have been the same without your support and friendship. I am excited to see what the years ahead hold for us!

Nowhere was teamwork more vital to my success than with this thesis. Dr. Kathryn Aten, thank you for encouraging me to pursue a grounded theory approach and helping me narrow my focus to something achievable. Dr. Chris Bellavita, your feedback from the intro class through this thesis was insightful and helped me crystalize my thoughts. Jennay Ghowrwal, thank you for taking the time to talk through my thesis and introducing me to the concept of "co-offending." Marianne Taflinger, you took the brunt of my passive voice, dependent-clause-first, instinctive writing style. Without your assistance, I am not sure anyone would have understood what I was trying to say.

I am also thankful for the three romance scam victims who participated in this study. Your willingness to share your experiences added depth to my findings. Hopefully,

some good will come out of this study so that fewer people will experience what you went through. Thank you for your time and candor.

Similarly, thank you to everyone who helped locate or tried to locate participants for this study. You are all busy professionals with multiple responsibilities. I appreciate that you took the time to try to help, even when your efforts did not lead to a participant enrolling.

Naturally, my team begins and ends with my family. I could neither have entered the program nor succeeded in it without your support. Here we are, though. I am done and frankly nervous that one or more of you kept a list of all the things I would do “once my thesis is done.” I love you all and thank you for making sacrifices so I could achieve this goal.

I. INTRODUCTION

According to the FBI's Internet Crime Complaint Center (IC3), the economic damage caused by cybercrime has risen sharply, increasing by 390%—from \$1.4 billion in 2017 to \$6.9 billion in 2021.¹ These crimes are perpetrated by individuals, transnational criminal organizations such as the Nigeria-based Black Axe, and adversarial nation-states like North Korea.² The FBI notes that offenders frequently use money laundering to conceal the proceeds of these frauds.³ One potential source of assistance with money laundering is romance scam victims, who may knowingly or unknowingly participate in the crime by transferring money, believing they are helping a loved one. By targeting romance scams, law enforcement can simultaneously disrupt criminals' ability to profit and launder money.

A. PROBLEM STATEMENT

"Every morning when I wake up the first thing hit my mind, is you. I close my eyes and picture your beautiful face in my head so I can start the day full of positivity. I feel lucky to have you in my life. You are a blessing that I will be thankful to God for the rest of my life," (AS2 to AV2.1 and AV2.7, November 2019). This script, found in archival communications between a suspect and two separate victims in this study, demonstrates the narratives constructed to defraud romance scam victims. According to reporting by the FBI, such romance scams cost over 24,000 Americans more than \$950 million in reported losses in 2021 alone.⁴

As if losing nearly a billion dollars is not bad enough, offenders sometimes induce romance scam victims to participate in laundering money stolen from other victims. The

¹ Federal Bureau of Investigation, *Internet Crime Report 2021* (Washington, DC: Federal Bureau of Investigation, 2022), 7, https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf.

² Africa Eye, "The Ultra-Violent Cult That Became a Global Mafia," BBC News, December 13, 2021, <https://www.bbc.com/news/world-africa-59614595>; United Nations, "Midterm Report of the Panel of Experts Submitted Pursuant to Resolution 2464 (2019)" (United Nations, August 30, 2019), 4, 110–12, https://www.un.org/securitycouncil/sanctions/1718/panel_experts/reports.

³ Federal Bureau of Investigation, "Don't Be a Mule," FBI News, December 17, 2018, <https://www.fbi.gov/news/stories/fbi-joins-international-campaign-to-stop-money-mules-121718>.

⁴ Federal Bureau of Investigation, *Internet Crime Report 2021*, 22–23.

FBI uses the term “money mule” to describe someone who “transfers or moves illegally acquired money on behalf of someone else.”⁵ Although research has explored romance scams and money mules independently, few studies feature romance scam victims as money mules. The small subset of money mules who continued to participate in money laundering after becoming aware that they were participating in a crime is of particular interest in this study. Investigators and policymakers require a better understanding of how criminals lead romance scam victims to participate in money laundering to reduce the financial risks posed to and by romance scam victims.

Scholars often categorize romance scams as a subset of advanced fee schemes.⁶ Although traditional advanced fee schemes involve the false promise of a large payout in exchange for an upfront payment, researcher Monica Whitty and others suggest suspects promise romance scam victims a relationship if only the victim could help the suspect financially through a series of purported crises keeping them apart.⁷ Whitty also finds suspects convince some romance scam victims, generally under false pretenses, to receive fraud proceeds from other cybercrimes and transfer them to another financial account at the suspect’s direction.⁸ Thus, the person could be both a victim and a co-conspirator.

Scholarly and practitioner literature has established the importance of money mules in laundering the over \$18.7 billion stolen from Americans via cybercrime between 2017 and 2021.⁹ For example, a report by Agari Data, an email security company, likens money

⁵ Federal Bureau of Investigation, “Money Mules,” Scams and Safety, accessed April 21, 2022, <https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/money-mules>.

⁶ Monica T. Whitty, “Do You Love Me? Psychological Characteristics of Romance Scam Victims,” *Cyberpsychology, Behavior, and Social Networking* 21, no. 2 (February 2018): 105, <https://doi.org/10.1089/cyber.2016.0729>; Alisdair A Gillespie, “The Electronic Spanish Prisoner: Romance Frauds on the Internet,” *The Journal of Criminal Law* 81, no. 3 (June 2017): 217–18, <https://doi.org/10.1177/0022018317702803>; Christian Kopp et al., “The Role of Love Stories in Romance Scams: A Qualitative Analysis of Fraudulent Profiles,” *International Journal of Cyber Criminology* 9, no. 2 (June 22, 2016): 207–9, <https://doi.org/10.5281/ZENODO.56227>.

⁷ Monica T. Whitty, “Anatomy of the Online Dating Romance Scam,” *Security Journal* 28, no. 4 (October 2015): 444, 446–48, <https://doi.org/10.1057/sj.2012.57>.

⁸ Whitty, 450.

⁹ Federal Bureau of Investigation, *Internet Crime Report 2021*, 7.

mules to “critical infrastructure” for money laundering operations.¹⁰ Likewise, researchers at Microsoft found that the limiting factor for monetizing stolen identities was not their scarcity; it was the number of available money mules.¹¹ Therefore, disrupting the recruitment and use of money mules should reduce cybercriminals’ abilities to profit from their crimes.

The body of literature addressing the phenomena of romance scams focuses on victim characteristics or the process of fraud. However, limited literature covers how suspects induce romance scam victims to collaborate as money mules in money laundering schemes. This thesis explores the process offenders use to guide some individuals through romance scam victimization and on to willingly participating in laundering money. This research has broad implications, from disrupting international organized crime groups and adversarial nation-states that use money mules, to shaping local law enforcement response to romance scam victims.

B. RESEARCH QUESTIONS

As previously illustrated, the ‘money mule’ aspect of romance scams remains under-researched. This study aims to understand the factors contributing to individuals becoming money mules after being victimized in online romance scams and to explore why some victims do not. To that end, this thesis intends to answer the following questions:

1. How do individuals become money mules after being victimized in online romance scams?
2. Why do all online romance scam victims not act as money mules?

¹⁰ Agari Cyber Intelligence Division, *The Geography of BEC: The Global Reach of the World’s Top Cyber Threat*, Threat Intelligence Brief (Foster City, CA: Agari Data, 2020), 11, <https://www.agari.com/cyber-intelligence-research/whitepapers/acid-agari-geography-of-bec.pdf>.

¹¹ Dinei Florencio and Cormac Herley, “Phishing and Money Mules,” in *2010 IEEE International Workshop on Information Forensics and Security* (2010 IEEE International Workshop on Information Forensics and Security, Seattle, WA: IEEE, 2010), 1–5, <https://doi.org/10.1109/WIFS.2010.5711465>.

C. ROMANCE SCAM LITERATURE REVIEW

Scant research delves deeply into the process that transforms romance scam victims into money mules. What does exist appears primarily in practitioner literature. This literature simply acknowledges that some romance scam victims act as money mules without describing or explaining how it occurs. Dr. Monica Whitty, one of the leading researchers into romance scams, mentions that romance scam victims sometimes aid money laundering scams by transferring money on behalf of criminals.¹² Likewise, Nicholls, Kuppa, and Le-Khac also document that fraudsters use romance scam victims to launder money in an article focused on using deep learning to combat cyber-enabled financial frauds.¹³ A study by Raza, Zhan, and Rubab mentions the recruitment of romance scam victims to act as money mules tangentially, asserting “this recruitment method is not commonly used.”¹⁴ Other than the passing references in these three articles, the scholarship addressing the process by which romance scam victims become money mules is sparse. This scarcity is particularly troubling because romance scams and money mule activity increased during the COVID-19 pandemic according to the FBI and research by Buil-Gil and Zeng.¹⁵ This review covers literature regarding romance scams.

The scholarly literature on romance scams reflects victim-centered, subject-centered, and prevention-centered approaches. The literature also contains some frameworks and scales for describing and measuring susceptibility to online scams. Scholars apply these frameworks and measures to romance scam victims, but do not extend them to the money mule phenomenon.

¹² Whitty, “Anatomy of the Online Dating Romance Scam,” 450.

¹³ Jack Nicholls, Aditya Kuppa, and Nhien-An Le-Khac, “Financial Cybercrime: A Comprehensive Survey of Deep Learning Approaches to Tackle the Evolving Financial Crime Landscape,” *IEEE Access* 9 (December 2021): 163977, <https://doi.org/10.1109/ACCESS.2021.3134076>.

¹⁴ Muhammad Subtain Raza, Qi Zhan, and Sana Rubab, “Role of Money Mules in Money Laundering and Financial Crimes a Discussion Through Case Studies,” *Journal of Financial Crime* 27, no. 3 (May 2020): 914, <https://doi.org/10.1108/JFC-02-2020-0028>.

¹⁵ “FBI Warns of Money Mule Schemes Exploiting the Covid-19 Pandemic,” April 6, 2020, <https://www.fbi.gov/news/pressrel/press-releases/fbi-warns-of-money-mule-schemes-exploiting-the-covid-19-pandemic>; David Buil-Gil and Yongyu Zeng, “Meeting You Was a Fake: Investigating the Increase in Romance Fraud During Covid-19,” *Journal of Financial Crime*, May 10, 2021, <https://doi.org/10.1108/JFC-02-2021-0042>.

1. Victim-Centered Romance Scam Studies

The victim-centered research, which comes primarily from studies in the UK and Australia, is split mainly between analyses of innate victim characteristics and descriptions of the victim's scam experience. The studies, including victims' inherent characteristics, seek to understand what personality traits make a person more susceptible to this fraud. Those focusing on the victims' experiences either seek to develop themes to better understand the fraud process or convey the scams' adverse effect on the victims. None of this research delves deeply into those victims who become money mules.

Studies profile the victims' personality traits to distinguish them from non-victims. Dr. Monica Whitty's significant contributions to the field have included numerous studies on victim characteristics.¹⁶ She finds victims of cyber scams, including romance scam victims, score higher on tests of neuroticism and impulsivity than non-victims.¹⁷ She also demonstrates that the victims are statistically more likely to be male, have an internal locus of control, and have higher education than non-victims.¹⁸ Whitty and Buchanan also find that romance scam victims score higher on the idealization subscale of the Romantic Beliefs Scale than users of dating websites who were not victims.¹⁹ Victims also tend to be more impulsive and have "addiction characteristics."²⁰ The overall findings establish measurable differences in personality traits between victims of romance scams and non-victims. However, as noted elsewhere, none of this research addresses the cohort of romance scam victims who ultimately serve as money mules.

¹⁶ Whitty, "Anatomy of the Online Dating Romance Scam"; Whitty, "Do You Love Me?"; Tom Sorell and Monica Whitty, "Online Romance Scams and Victimhood," *Security Journal* 32, no. 3 (September 2019): 342–61, <https://doi.org/10.1057/s41284-019-00166-w>; Monica T. Whitty, "Predicting Susceptibility to Cyber-Fraud Victimhood," *Journal of Financial Crime* 26, no. 1 (January 7, 2019): 277–92, <https://doi.org/10.1108/JFC-10-2017-0095>; M. T. Whitty, "The Scammers Persuasive Techniques Model: Development of a Stage Model to Explain the Online Dating Romance Scam," *British Journal of Criminology* 53, no. 4 (July 1, 2013): 665–84, <https://doi.org/10.1093/bjc/azt009>.

¹⁷ Monica Whitty, "Is There a Scam for Everyone? Psychologically Profiling Cyberscam Victims," *European Journal on Criminal Policy and Research* 26, no. 3 (September 2020): 407, <https://doi.org/10.1007/s10610-020-09458-z>.

¹⁸ Whitty, 407.

¹⁹ Tom Buchanan and Monica T. Whitty, "The Online Dating Romance Scam: Causes and Consequences of Victimhood," *Psychology, Crime & Law* 20, no. 3 (March 16, 2014): 281, <https://doi.org/10.1080/1068316X.2013.772180>.

²⁰ Whitty, "Do You Love Me?," 108.

The studies of the victims' experiences range from the singularly focused to attempts to model the entire ordeal. Whitty first developed an "anatomy" of the romance scam that she laid out in a "trajectory."²¹ Based on interviews with victims and a UK police officer, she describes victims proceeding from locating an attractive online dating profile, undergoing grooming by the offender, complying with a request for money, experiencing online sexual abuse (for some), and finally reaching an understanding of their victimization.²² Other studies of romance scams cite this trajectory and a subsequent model.

Cassandra Cross argues that frustrations about jurisdictional issues can cause victims to feel revictimized in reporting romance scams to the Australian police.²³ In separate works, Cross and Gillespie contend that romance scam victims suffer psychological distress to a high degree, similar to domestic violence or a sexual assault victim.²⁴ Gillespie expands his argument by asserting that romance scammers deserve more severe sentences than simple fraud offenders.²⁵ Several articles in this category conclude that perceived gullibility and participation in their victimization leads to victim-blaming.²⁶ Regardless of the focus, this body of research demonstrates that romance scam victims often experience psychological harm in addition to financial loss.

a. The Scammer's Persuasive Techniques Model

As noted elsewhere, Dr. Monica Whitty is a leading researcher studying romance scams. In 2013, she published two frequently cited articles containing models of romance

²¹ Whitty, "Anatomy of the Online Dating Romance Scam," 446.

²² Whitty, 446.

²³ Cassandra Cross, "'Oh We Can't Actually Do Anything About That': The Problematic Nature of Jurisdiction for Online Fraud Victims," *Criminology & Criminal Justice* 20, no. 3 (July 2020): 358–75, <https://doi.org/10.1177/1748895819835910>.

²⁴ Gillespie, "The Electronic Spanish Prisoner"; Cassandra Cross, Molly Dragiewicz, and Kelly Richards, "Understanding Romance Fraud: Insights from Domestic Violence Research," *The British Journal of Criminology* 58, no. 6 (October 5, 2018): 1303–22, <https://doi.org/10.1093/bjc/azy005>.

²⁵ Gillespie, "The Electronic Spanish Prisoner," 231.

²⁶ Sorell and Whitty, "Online Romance Scams and Victimhood"; Gillespie, "The Electronic Spanish Prisoner," 221; Cross, Dragiewicz, and Richards, "Understanding Romance Fraud," 1317.

scams.²⁷ The first report features a framework of romance scams derived from three qualitative studies.²⁸ One study collects and analyzes 200 romance scam victim stories from a website dedicated to the topic.²⁹ Whitty’s second study consists of field interviews of 20 romance scam victims: nineteen from the United Kingdom and one from the United States.³⁰ Her third study is an interview of a police officer in the United Kingdom considered an expert in investigating romance scams.³¹ Her analysis of these studies led to the development of her “Romance Scam Trajectories” model (see Figure 1).³² She describes the model as an “anatomy” of the scam, which includes “the profile,” “grooming,” “the sting,” “sexual abuse,” and “revelation” stages.³³

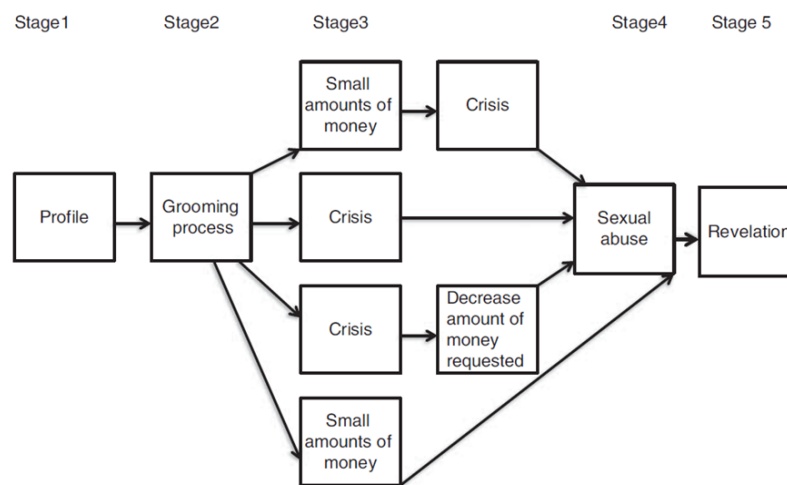


Figure 1. Romance Scam Trajectories³⁴

²⁷ Md Nabid Alam, “Three Essays on Socially Engineered Attacks: The Case of Online Romantic Scams” (PhD diss., University of North Carolina at Greensboro, 2021), 9, 21; Kopp et al., “S,” 209; Cross, Dragiewicz, and Richards, “Understanding Romance Fraud,” 1306; Guillermo Suarez-Tangil et al., “Automatically Dismantling Online Dating Fraud,” *IEEE Transactions on Information Forensics and Security* 15 (2020): 1128, <https://doi.org/10.1109/TIFS.2019.2930479>.

²⁸ Whitty, “Anatomy of the Online Dating Romance Scam,” 444–45.

²⁹ Whitty, 445.

³⁰ Whitty, 445.

³¹ Whitty, 445–46.

³² Whitty, 446.

³³ Whitty, 446–54.

³⁴ Source: Whitty, 446.

Whitty discusses money laundering by romance scam victims in the grooming stage of the article under the heading “turning victims into criminals.”³⁵ She reports “a handful of victims” involved in this behavior.³⁶ However, she does not incorporate money laundering into her overall model.

Later in 2013, Whitty published a second article focusing on the “persuasive techniques” used by romance scam offenders.³⁷ This article analyzes the same data gathered in her previous study involving interviewing 20 victims.³⁸ Whitty attempts to determine whether prior theories developed following investigations of mass marketing fraud, based on social psychology research, could be applied to romance scams.³⁹ She finds cognitive dissonance explains how victims accept some false premises as valid while ignoring conflicting information.⁴⁰ Whitty also asserts some victims continue to participate in a romance scam due to the “near-win phenomenon.”⁴¹ Finally, Whitty develops “The Scammers Persuasive Techniques Model” based on her findings (see Figure 2).⁴²

³⁵ Whitty, 450.

³⁶ Whitty, 450.

³⁷ Whitty, “The Scammers Persuasive Techniques Model.”

³⁸ Whitty, 669–71.

³⁹ Whitty, 666–69.

⁴⁰ Whitty, 682. Note: Whitty explains cognitive dissonance as an individual’s tendency to alleviate the tension caused by encountering information contrary to existing beliefs by rationalizing or using other mental methods.

⁴¹ Whitty, 682. Note: Whitty attributes the “near-win phenomenon” to gambling research, but it has been applied to mass marketing fraud. It is “a failure that comes close to being successful,”⁶⁷⁵.

⁴² Whitty, 677.

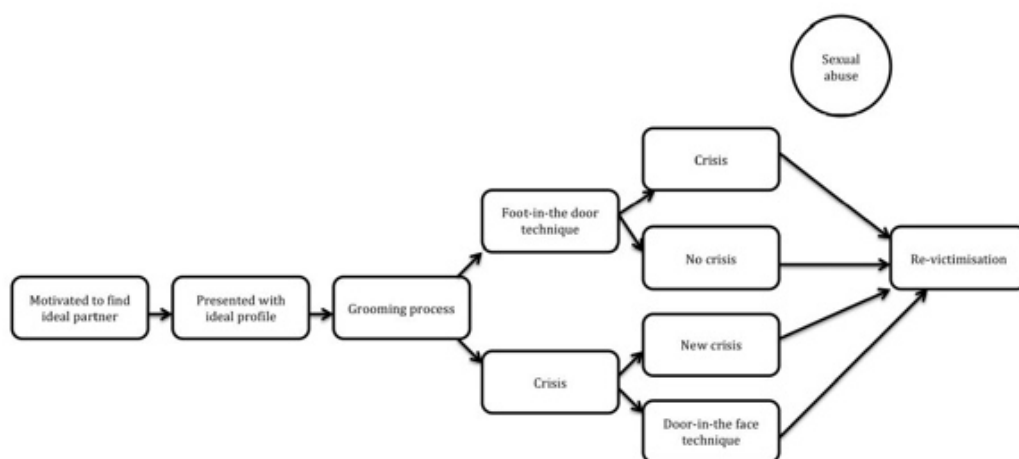


Figure 2. The Scammers Persuasive Techniques Model⁴³

Whitty claims The Scammers Persuasive Techniques Model “explains why individuals get hooked and how criminals manage to carefully groom individuals to a point where they are ready to part with their money.”⁴⁴ This model expands her original framework from five to seven stages: “motivated to find the ideal partner,” “presented with the ideal profile,” “grooming process,” “the sting,” “continuation of the scam,” “sexual abuse,” and “re-victimization.”⁴⁵ Citing previous research by J. Rusch and S. Lea et al., Whitty adopts some terminology from marketing theory, including the “foot-in-the-door technique” and the “door-in-the-face technique” to describe methods used by scammers.⁴⁶ The former involves small requests for money followed by larger ones. The latter entails soliciting an unreasonably large amount upfront, followed by apparently more reasonable, more minor requests.⁴⁷ Whitty describes the door-in-the-face technique as an alternative tactic offenders use following a refusal of prior requests for money.⁴⁸ She neither mentions money laundering by romance scam victims in this article nor builds it into her model.

⁴³ Source: Whitty, 677.

⁴⁴ Whitty, 682.

⁴⁵ Whitty, 676–81.

⁴⁶ Whitty, 667, 679–80.

⁴⁷ Whitty, 679–80.

⁴⁸ Whitty, 680.

b. *Alam's Study of Romance Scams*

In his doctoral dissertation, Md Nabid Alam drew from existing psychological research to construct a study that measured the effect of relationship satisfaction, relationship trust, “love seeking status,” and mood congruence on gullibility to romance scams.⁴⁹ Alam presented the study participants with one of four randomly assigned vignettes. The vignettes contained 1) no grooming language, 2) intimacy language only, 3) intimacy and passion language, or 4) intimacy, passion, and commitment language.⁵⁰ Alam adapted various scripts from real-life scams listed on a website dedicated to romance scams.⁵¹ After reading the vignette, the participants answered questions designed to measure relationship satisfaction and trust. Alam concludes that grooming by a scammer, including intimacy, passion, and commitment, predicts increased susceptibility to being scammed by affecting the participants’ level of trust and satisfaction in the relationship. Commitment language demonstrates a more powerful effect than passion and intimacy language.⁵² Alam describes intimacy, passion, and commitment as follows:

Intimacy in a relationship is a feeling of being close, emotionally connected, and supported. It also means regular and meaningful communications. Passion in a relationship is an intense feeling of love, affection, and desire. Commitment in a relationship refers to whether there is understanding about the future and whether the partners see each other together in the long run.⁵³

Alam drew heavily on the work of Robert Sternberg at Yale University to create the definitions he used for intimacy, passion, and commitment.⁵⁴ Sternberg used these terms when advancing “A Triangular Theory of Love.”⁵⁵ In Sternberg’s view, “the

⁴⁹ Alam, “Three Essays on Socially Engineered Attacks,” 10–11.

⁵⁰ Alam, 73.

⁵¹ Alam, 73.

⁵² Alam, 81.

⁵³ Alam, 193.

⁵⁴ Alam, 65.

⁵⁵ Robert J. Sternberg, “A Triangular Theory of Love,” *Psychological Review* 93, no. 2 (April 1986): 119–35, <https://doi.org/10.1037/0033-295X.93.2.119>.

different possible combinations of intimacy, passion, and decision/commitment,” explain the varied experience we define as “love.”⁵⁶

Though conducted in a lab and not in the field on actual scam victims, Alam’s research provides empirical measures of the effects of specific language commonly used by offenders on a person’s potential susceptibility to a romance scam. Like previous research, it does not address nor differentiate the grooming experienced by the subset of romance scam victims who become money mules.

2. Subject-Centered Romance Scam Studies

The subject-centered research on romance scams focuses on the perpetrator or the modus operandi. Research centered on the perpetrators themselves seeks to explain the motivations and rationalizations for engaging in this type of cyber-fraud.⁵⁷ The studies examining modus operandi include those that conduct textual analysis of the language used by the perpetrator while grooming the victim to fulfill a request for money willingly.⁵⁸ Regardless of the focus, subject-centered research aims to develop means to reduce these crimes.

3. Prevention-Centered Romance Scam Studies

Numerous articles, directly and indirectly, address methods to prevent online dating fraud. Most of these articles propose or test technological solutions to the problem. Existing research focuses on using artificial intelligence, machine learning, or deep learning to

⁵⁶ Sternberg, 132.

⁵⁷ Samuel O. Adejoh et al., “‘Yahoo Boys’ Phenomenon in Lagos Metropolis: A Qualitative Investigation,” *International Journal of Cyber Criminology* 13, no. 1 (June 2019), <https://doi.org/10.5281/ZENODO.3366298>; Jonathan Nii Barnor Barnor et al., “Rationalizing Online Romance Fraud: In the Eyes of the Offender,” *AMCIS 2020 Proceedings* 21: 12, accessed March 5, 2022, https://www.researchgate.net/profile/Emmanuel-Kolog/publication/343392445_Rationalizing_Online_Romance_Fraud_In_the_Eyes_of_the_Offender/links/5f31381092851cd302ec0508/Rationalizing-Online-Romance-Fraud-In-the-Eyes-of-the-Offender.pdf.

⁵⁸ Elisabeth Carter, “Distort, Extort, Deceive and Exploit: Exploring the Inner Workings of a Romance Fraud,” *The British Journal of Criminology* 61, no. 2 (February 26, 2021): 283–302, <https://doi.org/10.1093/bjc/azaa072>; Kopp et al., “S.”

identify fraudulent online dating profiles via profile images or the texts employed by suspects.⁵⁹

Scholars have researched several promising computer-aided techniques. One paper by Cross and Michael Kelly examines the effectiveness of prevention messaging in stopping online scams, including romance frauds.⁶⁰ They argue that prevention messaging is overly complex and does not target the primary concern, the victim's recognition of a fraudulent request for money or personal information.⁶¹ Another article by Cross and Rebecca Layt studies the utility of internet searches by victims to detect fraudulent profiles.⁶² Finally, in a novel study, researchers at Georgia State University targeted creators of fake dating profiles to test whether emails containing warnings could discourage their fraudulent activities.⁶³ These studies contribute to understanding how cyber-defenses may mitigate online romance frauds.

However, some scholars expressed concern that cybersecurity measures may hamper the legitimate use of a platform by real users. For instance, Chua et al. contend that requiring users of dating platforms to confirm their identity would give the platform the users' identifiers and knowledge about sexual preferences that the user would prefer not to

⁵⁹ Suarez-Tangil et al., "Automatically Dismantling Online Dating Fraud"; Xinlei He et al., "DatingSec: Detecting Malicious Accounts in Dating Apps Using a Content-Based Attention Network," *IEEE Transactions on Dependable and Secure Computing* 18, no. 5 (2021): 2193–2208, <https://doi.org/10.1109/TDSC.2021.3068307>; Nicholls, Kuppa, and Le-Khac, "Financial Cybercrime"; Suhaib Al-Rousan et al., "Social-Guard: Detecting Scammers in Online Dating," in *2020 IEEE International Conference on Electro Information Technology (EIT)* (2020 IEEE International Conference on Electro Information Technology (EIT), Chicago, IL, USA: IEEE, 2020), 416–22, <https://doi.org/10.1109/EIT48999.2020.9208268>.

⁶⁰ Cassandra Cross and Michael Kelly, "The Problem of 'White Noise': Examining Current Prevention Approaches to Online Fraud," *Journal of Financial Crime* 23, no. 4 (October 3, 2016): 806–18, <https://doi.org/10.1108/JFC-12-2015-0069>.

⁶¹ Cross and Kelly, 816.

⁶² Cassandra Cross and Rebecca Layt, "'I Suspect That the Pictures Are Stolen': Romance Fraud, Identity Crime, and Responding to Suspicions of Inauthentic Identities," *Social Science Computer Review*, March 2021, <https://doi.org/10.1177/0894439321999311>.

⁶³ Fangzhou Wang et al., *The Restrictive Deterrent Effect of Warning Messages Sent to Active Romance Fraudsters: An Experimental Approach* (Atlanta: CrimRxiv, 2020), <https://doi.org/10.21428/cb6ab371.c6eae022>.

share.⁶⁴ Suarez-Tangil et al. conclude that automated systems can deny legitimate users access to a dating site due to similarities between genuine and scam profiles.⁶⁵ These articles object to the use of overly broad approaches that would inhibit legitimate user engagement on the platforms.

D. OVERVIEW OF MONEY LAUNDERING

An understanding of money laundering and the role money mules play in it is necessary to fully appreciate the danger money mules pose. The financial system is set up to carefully record transactions so they can be tracked from beginning to end. Experts assert that the trail created by these records is exactly what money launderers are trying to conceal or confuse.⁶⁶ Thus, money laundering is the process of making the proceeds of crime appear legitimate. Criminals engage in money laundering in an effort to avoid detection by law enforcement.

1. The Money Laundering Cycle

According to John Madinger in *Money Laundering: A Guide for Criminal Investigators*, money laundering has three steps: placement, layering, and integration.⁶⁷ Madinger explains that during the placement stage, the illegal money is entered into the financial system. Next, distance is placed between the crime and the money by conducting a series of transactions. Layers are thereby erected between the illegal activity and the money itself. Lastly, the source of the money is made to appear legitimate through various

⁶⁴ Yi Ting Chua et al., “Identifying Unintended Harms of Cybersecurity Countermeasures,” in *2019 APWG Symposium on Electronic Crime Research (eCrime)* (2019 APWG Symposium on Electronic Crime Research (eCrime), Pittsburgh, PA: IEEE, 2019), 5, <https://doi.org/10.1109/eCrime47957.2019.9037589>.

⁶⁵ Suarez-Tangil et al., “Automatically Dismantling Online Dating Fraud,” 1135.

⁶⁶ John Madinger, *Money Laundering: A Guide for Criminal Investigators*, 3rd ed (Boca Raton, FL: Taylor & Francis, 2012), 5. Note: the money laundering section is adapted from “Hushing Lazarus: A Case Study of the Money Laundering Conspiracy Involving Members of the North Korean Army’s Lazarus Group, the Instagrammer ‘Hushpuppi,’ and others” written for Dr. Chris Bellavita and Dr. Lauren Fernandez’s Introduction to Homeland Security Course.

⁶⁷ Madinger, 5–6.

schemes such as fake loans, contracts, shell companies, and insurance products. Madinger elaborates that this integration of the proceeds into the legitimate economy enables the suspect to spend the money with less fear that the government will learn of its illegal source.

2. The Bank Secrecy Act and USA PATRIOT Act

Through the Bank Secrecy Act (BSA), and subsequent related acts, Congress has sought to provide the Treasury Department, law enforcement, and other governmental entities with the tools to combat money laundering and other crimes that exploit the U.S. financial sector.⁶⁸ Table 1 shows some of the reports that financial institutions and others are required to file to maintain compliance with the BSA. Under the BSA, the Treasury Secretary has the authority to promulgate rules and specify entities that constitute a “financial institution.” According to Madinger, the Secretary’s authority to define financial institutions and ensuing legislation passed by Congress have led to a schema where businesses far beyond banks are required to file reports under the BSA.⁶⁹ These businesses currently include jewelers, casinos, hawala, cryptocurrency companies, and will soon include arts and antiquities dealers.⁷⁰

⁶⁸ “BSA Timeline | FinCEN.Gov,” accessed November 20, 2021, <https://www.fincen.gov/resources/statutes-regulations/bank-secrecy-act/bsa-timeline>.

⁶⁹ Madinger, *Money Laundering*, 57–58.

⁷⁰ “BSA Timeline | FinCEN.Gov”; “Anti-Money Laundering Regulations for Dealers in Antiquities” (Federal Register, September 24, 2021), 53021–24, <https://www.govinfo.gov/content/pkg/FR-2021-09-24/pdf/2021-20731.pdf>.

Table 1. Select Bank Secrecy Act Report Types⁷¹

Report Name	Description
<i>Currency Transaction Reports (CTR)</i>	Filed by financial institutions on all currency transactions over \$10,000.
<i>Currency and Monetary Instrument Report (CMIR)</i>	Filed by a person involved in moving currency with a value over \$10,000 across the U.S. border.
<i>Form 8300 (8300)</i>	Filed by business owners who receive over \$10,000 in cash from a customer.
<i>Suspicious Activity Reports (SAR)</i>	Filed by financial institutions and provides the who, what, when, where, and why of suspicious transactions that may or may not have been captured by other reporting.

Following the passage of the USA PATRIOT Act in October 2001, financial institutions were required to have a Customer Identification Program.⁷² In his book on money laundering, Chris Mathers explains this program is referred to as “Know Your Customer” (KYC).⁷³ The concept behind KYC, according to Mathers, is that financial institutions should know with whom they are doing business. That knowledge should include basic biographical information, why the account is being opened, and the expected types of transactions. Mathers asserts that this background information makes it easier for banks to detect fraud by or against the customer and report it to law enforcement.⁷⁴

3. Money Laundering and the BSA

As previously noted, the goal of money laundering is to obfuscate the suspect behind the illegal financial transaction in the hope that they will be able to spend the criminal proceeds without drawing undue attention. Success in this endeavor includes

⁷¹ Adapted from Madinger, *Money Laundering*, 59–62.

⁷² “Customer Identification Program Requirements for Banks,” 31 CFR § 1020.220, accessed November 20, 2021, <https://www.law.cornell.edu/cfr/text/31/1020.220>.

⁷³ Chris Mathers, *Crime School: Money Laundering* (Buffalo, NY: Firefly Books, 2004), 125.

⁷⁴ Mathers, 126.

avoiding BSA reporting. Money launderers employ a variety of techniques to accomplish this objective.

For instance, Madinger reports money launderers sometimes split cash deposits up, so the transactions stay under the \$10,000 threshold for a CTR filing and the related collection of the KYC data by the bank.⁷⁵ They may do this by visiting several branches of the same bank themselves or making smaller transactions over consecutive days. Madinger states that banks monitor for this practice, which is a crime known as “structuring.”⁷⁶

If a bank suspects structuring, it will likely file a SAR. Therefore, money launderers will sometimes employ multiple people to conduct these transactions. According to Mathers, this activity is called “smurfing.”⁷⁷ Banks also monitor for smurfing and file CTRs if the aggregate deposit to an account is over \$10,000 cash in 24 hours. Consequently, money launderers may open multiple accounts and transfer funds between them.

Money launderers also must circumvent KYC rules. If the beneficial owner of an account that received criminal proceeds can be identified, the suspect can be more easily tied to a crime. Thus, experts report money launderers sometimes open accounts using stolen identities, fake identities, or a combination of the two, known as synthetic identities.⁷⁸

Experts tell us money launderers use straw buyers to mitigate the threats of detection that 8300s present to suspects.⁷⁹ In a money laundering scheme, a straw buyer makes a purchase on behalf of another person using criminal proceeds. If the business

⁷⁵ Madinger, *Money Laundering*, 59–60.

⁷⁶ Madinger, 59.

⁷⁷ Mathers, *Crime School*, 149.

⁷⁸ Lukayn Hunsicker, “Everything Financial Institutions Need to Know about Synthetic Identity Fraud – Thomson Reuters Institute,” Thomson Reuters, December 1, 2020, <https://www.thomsonreuters.com/en-us/posts/investigation-fraud-and-risk/synthetic-identity-fraud/>.

⁷⁹ The Swartz Law Firm, “Hiding Cash Payments from the IRS for Luxury Car Purchases Resulted in Conviction,” *Swartz Law Firm Civil & Criminal Trial Law* (blog), November 26, 2018, <https://www.whitecollarcriminaldefenselawyerblog.com/hiding-cash-payments-from-the-irs-for-luxury-car-purchases-resulted-in-conviction/>.

receiving the funds files an 8300, the person named will be the straw buyer, not the criminal. Thus, the criminal derives an extra layer of protection from discovery.

4. Money Mules

Money launderers can use money mules to solve many of the problems the BSA poses for them. The Financial Action Task Force (FATF), an inter-governmental organization focused on anti-money laundering, reports that money mules are persons who illegally move the proceeds of crime on behalf of professional money launderers or organized crime groups.⁸⁰ According to the FATF, they can be unwitting, witting, or complicit accomplices to the overall money laundering scheme.⁸¹ Complicit money mules intentionally aid the money launderer, while unwitting ones do so unintentionally. Witting money mules land in between complicit and unwitting. The FATF maintains that witting participants turn a blind eye to the suspicious activity they observe.⁸² Money mules are primarily involved in the placement and layering stages of a money-laundering scheme. Like straw buyers, they add an obscuring layer between the crime and the criminal.

a. Moving Money

Regardless of their level of knowledge of the scheme, the money mule's role is to participate in the transfer of value through the financial system from the victim to the suspect that initiated the cyber-attack.⁸³ There are as many different ways to accomplish this goal as there are ways to send money or valuable commodities.

One practice gaining prominence is the offender directing the mule to withdraw fraudulently obtained proceeds in cash and deposit them at a Bitcoin ATM. The U.S. Treasury Financial Crimes Enforcement Network (FinCEN) reports that once the proceeds

⁸⁰ Financial Action Task Force, *Professional Money Laundering* (Paris: Financial Action Task Force (FATF), 2018), 22, www.fatf-gafi.org/publications/methodandtrends/documents/professional-money-laundering.html.

⁸¹ Financial Action Task Force, 22.

⁸² Financial Action Task Force, 23.

⁸³ Financial Action Task Force, 22.

are in the form of cryptocurrency, they can be easily transferred around the globe.⁸⁴ The offender can also layer cryptocurrency using mixers and peel chains, a discussion of which is beyond the scope of this thesis. Still, money launderers' use of cryptocurrency demonstrates that they will adapt their techniques to transfer value via money mules as new technologies emerge.

Money mules may open domestic or international bank accounts. These accounts aid in the placement and layering phases of the money laundering scheme by providing destinations for electronic and cash transfers. FinCEN reported in 2019 that most of the initial transfers of fraud proceeds were to domestic bank accounts and assessed that criminal groups were taking advantage of money mule networks.⁸⁵ The FATF asserts money mule networks are frequently operated by transnational organized crime groups involved in cybercrime.⁸⁶ Ultimately, domestic money mules assist in the international movement of fraud proceeds, according to an FBI statement.⁸⁷

b. Links to Cybercrime and Cyber-enabled Crime

Though the terms are often used interchangeably, the International Criminal Police Organization (Interpol) advances different definitions for cybercrime and cyber-enabled crime. Interpol classifies cyber-enabled crime as “traditional” crimes committed via electronic means such as frauds or swindles.⁸⁸ Cybercrimes, by comparison, are those crimes that involve “sophisticated attacks, or high-tech crimes” according to Interpol, such as ransomware or hacking.⁸⁹ The primary difference between the two is the amount of technical skill needed to complete the crime.

⁸⁴ Financial Crimes Enforcement Network, “Advisory on Illicit Activity Involving Convertible Virtual Currency” (Financial Crimes Enforcement Network (FinCEN), May 9, 2019), 4, <https://www.fincen.gov/resources/advisories/fincen-advisory-fin-2019-a003>.

⁸⁵ Financial Crimes Enforcement Network, *Updated Advisory on Email Compromise Fraud Schemes Targeting Vulnerable Business Processes* (Financial Crimes Enforcement Network (FinCEN), 2019), <https://www.fincen.gov/resources/advisories/fincen-advisory-fin-2019-a005>.

⁸⁶ Financial Action Task Force, *Professional Money Laundering*, 22.

⁸⁷ Federal Bureau of Investigation, “Don’t Be a Mule.”

⁸⁸ Interpol, “Cybercrime” (Interpol), 4, accessed October 25, 2021, <https://www.interpol.int/content/download/5267/file/Cybercrime.pdf>.

⁸⁹ Interpol, 4.

The FBI and FinCEN report that a large percentage of transactions conducted by money mules are linked to cybercrime and cyber-enabled crime, such as romance scams, lottery scams, business email compromise (BEC), ransomware, and phishing.⁹⁰ The University of Lagos’ Ehi Eric Esoimeme referenced reports from European law enforcement that over 90% of money mule transactions “are linked to cybercrime.”⁹¹ The FATF added in a report on professional money laundering that money mule accounts are “highly effective in laundering funds.”⁹² The report goes on to state that these money mule networks are often associated with international organized cybercriminal groups.

Just as money mule networks do not move money for only one type of cyber-enabled fraud, they do not always work with a single criminal enterprise. The FATF reported that multiple organized crime groups may use the same money mule network.⁹³ Thus, a single money mule may move fraud proceeds from various scams for different suspects.

c. Prevalence of Money Mules

Likely several thousand people are operating as money mules in the U.S. at any given time. Terrill Caplan, an expert on West African organized crime, was cited in a Better Business Bureau report, estimating that 20 to 30% of romance scam victims in 2018 were lured into money mule activity.⁹⁴ That same year, the FBI’s Internet Crime Complaint Center (IC3) received 18,493 complaints involving romance and confidence scams.⁹⁵ If

⁹⁰ Federal Bureau of Investigation, “Don’t Be a Mule”; Financial Crimes Enforcement Network, *Updated Advisory on Email Compromise Fraud Schemes Targeting Vulnerable Business Processes*.

⁹¹ Ehi Eric Esoimeme, “Identifying and Reducing the Money Laundering Risks Posed by Individuals Who Have Been Unknowingly Recruited as Money Mules,” *Journal of Money Laundering Control* 24, no. 1 (May 2021): 203, <https://doi.org/10.1108/JMLC-05-2020-0053>.

⁹² Financial Action Task Force, *Professional Money Laundering*, 23.

⁹³ Financial Action Task Force, 25.

⁹⁴ Better Business Bureau, “Fall in Love, Go to Jail: BBB Report on How Some Romance Fraud Victims Become Money Mules,” Latest News, February 15, 2019, <https://www.bbb.org/article/news-releases/19398-fall-in-love-go-to-jail-bbb-report-on-how-some-romance-fraud-victims-become-money-mules>.

⁹⁵ Federal Bureau of Investigation, “2018 Internet Crime Report,” April 22, 2019, 19, <https://www.ic3.gov/Home/AnnualReports>.

Caplan's estimates are accurate, that would mean between 3,699 and 5,548 people operated as money mules following victimization in romance scams in 2018.

Other data similarly indicates that the number of money mules is in the thousands. The U.S. Department of Justice (DOJ) reported it took enforcement action against over 2,300 money mules during a money mule initiative in October and November 2020.⁹⁶ DOJ found money mules in every U.S. state during this enforcement action. Esoimeme relayed that 3,833 money mules were identified in a similar campaign by European law enforcement agencies targeted at money mules in a three month period in 2019.⁹⁷ Having a large number of geographically dispersed money mules offers offenders a myriad of ways to confuse the trail of fraudulent funds from victims to themselves.

E. CONTRIBUTION

This thesis builds on prior works on romance scams, gullibility, and co-offending.⁹⁸ In Chapter V, I offer a model of how offenders groom individuals for exploitation as scam victims and money mules by using personas the victims perceive as romantic partners. This model is grounded in the data I collected and is connected to prior research. I also propose a grounded theory explaining how the interactions in the model can result in an individual proceeding through a romance scam and on to knowingly participating in money laundering as a co-offender. Similarly, I suggest a new definition of *grooming* in the context of online romance scams based on the data in this study and prior related research. The model, theory, and definition are together intended to advance our understanding of money mules in the context of romance scams.

⁹⁶ Department of Justice, "U.S. Law Enforcement Takes Action Against Approximately 2,300 Money Mules In Global Crackdown On Money Laundering," Justice News, December 2, 2020, <https://www.justice.gov/opa/pr/us-law-enforcement-takes-action-against-approximately-2300-money-mules-global-crackdown-money>.

⁹⁷ Esoimeme, "Identifying and Reducing the Money Laundering Risk," 205.

⁹⁸ "Co-offending is easily defined as committing criminal acts with more than one offender." Kenethia L. McIntosh Fuller, "Personality and Crime: An Examination of the Influence of the Five Factor Model on Offending and Co-Offending" (PhD diss., Indiana University of Pennsylvania, 2012), 6.

Further, this thesis adds to the growing library of works at Naval Postgraduate School (NPS) revolving around homeland security issues in cyberspace. Ryan Monaghan's thesis "Cybercrime Response Capabilities and Capacity: An Evaluation of Local Law Enforcement's Response to a Complex Problem" is relevant to this thesis because Monaghan discusses local police departments' abilities to respond to crimes in cyberspace.⁹⁹ Eric Rosner's thesis, titled "Cyber Federalism: Defining Cyber's Jurisdictional Boundaries," tackles the significant hurdle of law enforcement jurisdiction in cyberspace.¹⁰⁰ Joseph Sembler's thesis on cryptocurrency describes how value is transferred via cryptocurrency, which was a method money mules employed in this study.¹⁰¹ Finally, Madison Miller's thesis on the metaverse shows us where romance scams will likely occur in the future.¹⁰² Gillespie asserts that romance scams have been around since at least the 1500s.¹⁰³ These scams have evolved through mailing letters, the fax machine, and into cyberspace. There is no reason to suspect romance scams will not continue into the metaverse if they have not already done so. This potential brings the importance of Monaghan's research into stark relief, because the metaverse transformed cyberspace before law enforcement fully adapted to cyberspace operations.

⁹⁹ Ryan M Monaghan, "Cybercrime Response Capabilities and Capacity: An Evaluation of Local Law Enforcement's Response to a Complex Problem" (master's thesis, Naval Postgraduate School, 2020), <https://www.hsdl.org/?view&did=850258>.

¹⁰⁰ Eric Rosner, "Cyber Federalism: Defining Cyber's Jurisdictional Boundaries" (master's thesis, Naval Postgraduate School, 2017), <https://www.hsdl.org/?view&did=808202>.

¹⁰¹ Joseph Sembler, "Cryptocurrency: Changing the Game for State and Local Law Enforcement" (master's thesis forthcoming, Naval Postgraduate School, 2023).

¹⁰² Madison Miller, "To Boldly Go Where No Metaverse Has Gone Before: A Virtual Reality Check" (master's thesis forthcoming, Naval Postgraduate School, 2023).

¹⁰³ Gillespie, "The Electronic Spanish Prisoner," 218.

THIS PAGE INTENTIONALLY LEFT BLANK

II. METHODS

I chose a grounded theory approach to answer this thesis' questions: "How do individuals become money mules after being victimized in an online romance scam?" and "Why do all romance scam victims not act as money mules?" Barney Glaser and Anselm Strauss assert that grounded theory "facilitates the generation of theories of process."¹⁰⁴ Gehman et al. similarly maintain that grounded theory is well suited to answering "how" questions.¹⁰⁵ First introduced in 1967 by Glaser and Strauss, grounded theory is an inductive approach to qualitative research.¹⁰⁶ It is intended to capture the lived experience of the people who directly participated in the phenomenon of interest.¹⁰⁷ In grounded theory, data is collected, analyzed, and used for theory generation. This approach contrasts with typical empirical studies that first assert a hypothesis and then collect data to confirm or deny the hypothesis. Therefore, I determined the grounded theory method fit the study's goals.

Over time, different approaches to the generation of grounded theory have emerged, and researchers debate their various merits.¹⁰⁸ Despite these variations, Corbin and Strauss maintain that all the approaches share "the 'constant comparative' method of analysis, the use of concepts and their development, theoretical sampling, and saturation."¹⁰⁹ I included each of these procedures in my research.

Coding is a process commonly used in grounded theory and other qualitative research to develop and label concepts found in the data. According to Thomas Schwandt in *The SAGE Dictionary of Qualitative Inquiry*, "coding is a procedure that disaggregates

¹⁰⁴ Barney G. Glaser and Anselm L. Strauss, *The Discovery of Grounded Theory: Strategies for Qualitative Research*, 5th ed. (New York: Aldine Publishing Company, 2010), 114.

¹⁰⁵ Joel Gehman et al., "Finding Theory–Method Fit: A Comparison of Three Qualitative Approaches to Theory Building," *Journal of Management Inquiry* 27, no. 3 (July 2018): 287, <https://doi.org/10.1177/1056492617706029>.

¹⁰⁶ Glaser and Strauss, *The Discovery of Grounded Theory*.

¹⁰⁷ Gehman et al., "Finding Theory–Method Fit," 296.

¹⁰⁸ Gehman et al., "Finding Theory–Method Fit."

¹⁰⁹ Juliet M. Corbin and Anselm L. Strauss, *Basics of Qualitative Research: Techniques and Procedures for Developing Grounded Theory*, 3rd ed. (Los Angeles: SAGE, 2008), 6.

the data, breaks it down into manageable segments, and identifies or names those segments.”¹¹⁰ Schwandt explains that coding should be a flexible process designed to describe or comprehend the studied phenomenon.¹¹¹ Glaser and Strauss suggest it may be best to totally “ignore the literature” on the topic of interest in order to generate the best-fitting codes for the data.¹¹² However, Schwandt reports codes can be generated deductively by first examining prior theories, inductively by developing codes directly from the data, or by a combination of both.¹¹³ As described later in this chapter, I combined deductive and inductive approaches to code development.

Constant comparison is a hallmark of the grounded theory method and consists of four parts. First, Glaser and Strauss advise that researchers should compare new codes with codes in other categories. They maintain that doing so will help elucidate the theoretical features of the codes.¹¹⁴ Glaser and Strauss then propose that codes should be integrated. By integrating related codes, the researcher begins to develop the theoretical connections between them.¹¹⁵ The third step involves defining the boundaries of the concepts and the theory. This step includes the “reduction” of the coded categories into “higher level concepts.”¹¹⁶ This reduction contributes to theory generation by promoting the development of terms that may be generalizable to instances beyond the topic being researched.¹¹⁷ Finally, Glaser and Strauss advocate the creation of a theory based on the reduced concepts.¹¹⁸ Here, they propose researchers may look to other studies focused on similar or diverse topics to develop a formal theory. Thus, the constant comparative method is a roadmap from coding to theory generation.

¹¹⁰ Thomas A. Schwandt, *The SAGE Dictionary of Qualitative Inquiry*, 4th ed. (Los Angeles: SAGE, 2015), 30.

¹¹¹ Schwandt, 31.

¹¹² Glaser and Strauss, *The Discovery of Grounded Theory*, 37.

¹¹³ Schwandt, *The SAGE Dictionary of Qualitative Inquiry*, 30–31.

¹¹⁴ Glaser and Strauss, *The Discovery of Grounded Theory*, 106.

¹¹⁵ Glaser and Strauss, 109.

¹¹⁶ Antony Bryant and Kathy Charmaz, *The SAGE Handbook of Grounded Theory* (Los Angeles: SAGE, 2007), 110.

¹¹⁷ Glaser and Strauss, *The Discovery of Grounded Theory*, 110–11.

¹¹⁸ Glaser and Strauss, 115.

Theoretical sampling in grounded theory consists of sampling to help generate or refine the theory the researcher is developing. Schwandt states that theoretical sampling occurs iteratively, with researchers selecting new samples based on the emerging theory and using them to generate new insights and further develop the theory.¹¹⁹ Glaser and Strauss report that theoretical sampling is used to fill gaps in the emerging theory.¹²⁰ Researchers repeat this process until the theory is saturated. Glaser and Strauss contend that theoretical saturation is achieved when the coding of new incidents provides no new insights.¹²¹ Theoretical sampling allows for the theory to be built inductively, from the data itself, rather than starting with a preconceived theory and trying to fit the data to it.

Throughout the process of interviewing participants and coding, grounded theory researchers write memos. In grounded theory, memos are more than just incident logs. Lora Lempert asserts memos are “complex research tools” that “conceptualize the data in narrative form.”¹²² Glaser and Strauss emphasize that researchers should write memos whenever they find themselves reflecting on the theoretical connections within and between the categories they are coding.¹²³ Memos, then, are an important tool for theory building.

Corbin and Strauss maintain that memos also aid researchers in reducing bias.¹²⁴ In grounded theory, the researcher is understood to be part of the process. Sara Diaz wrote in her NPS thesis that “grounded theory accepts the background and perspective of the researcher as an integral part of the research process.”¹²⁵ However, acceptance of the researcher’s perspective is not an excuse for bias. Thus, Corbin and Strauss advocate

¹¹⁹ Schwandt, *The SAGE Dictionary of Qualitative Inquiry*, 63.

¹²⁰ Glaser and Strauss, *The Discovery of Grounded Theory*, 109.

¹²¹ Glaser and Strauss, 111.

¹²² Lora Bex Lempert, “Asking Questions of the Data: Memo Writing in the Grounded Theory Tradition,” in *The Sage Handbook of Grounded Theory*, ed. Antony Bryant and Kathy Charmaz (Los Angeles: SAGE, 2007), 2.

¹²³ Glaser and Strauss, *The Discovery of Grounded Theory*, 107.

¹²⁴ Corbin and Strauss, *Basics of Qualitative Research*, 7.

¹²⁵ Sara Katherine Diaz, “Where Do I Start? Decision Making in Complex Novel Environments” (master’s thesis, Naval Postgraduate School, 2010), 16, <http://hdl.handle.net/10945/5132>.

techniques like memo-writing to help the researcher recognize biases if they form.¹²⁶ Therefore, I continually wrote memos throughout the process of collecting and analyzing the data in order to develop theoretical insights and watch for bias.

A. FIELD INTERVIEW CASES

Interviews are a common method to collect data in grounded theory research. Therefore, I elected to seek out study participants who had been victimized in romance scams and became money mules. Because the secondary question, “Why do all online romance scam victims not act as money mules?” was one of variance, I decided that all adult victims of online romance scams would be eligible for the study. I believed theoretical understanding of the process undergone by money mules would be enhanced by comparing them to victims who did not become money mules. Since the research involved human subjects, I sought and received prior approval from NPS’ Institutional Review Board (IRB). I began recruiting participants following the IRB’s approval of the research in August 2022.

1. Recruitment Efforts

I employed intermediaries to recruit study participants. If money mules, specifically those who had knowingly assisted in money laundering efforts, were identified, it was possible they would be revealing their participation in criminal acts that were unknown to law enforcement. While I anonymized all data, I could not assure complete confidentiality. Therefore, I used third parties. I collected human subjects data only after a person had provisionally agreed to participate in the study.

I first crafted an email introducing the study with the IRB-approved recruitment script attached. The email requested recipients provide the recruitment script to potentially eligible participants. Email recipients were asked not to provide me with the potential participant’s contact information. I emphasized that participants would need to contact me of their own volition. Recipients were also encouraged to forward the original email to others who could assist with recruitment.

¹²⁶ Corbin and Strauss, *Basics of Qualitative Research*, 7.

The first recruitment effort targeted 34 individuals employed in private industry, local law enforcement, federal law enforcement, criminal prosecution, non-governmental organizations, fusion centers, and regulatory agencies. The email recipients were located in at least ten states. I sent the first emails on August 30, 2022.

In addition to email recruitment, I contacted local law enforcement officers in Minnesota and an employee of a Minnesota regulatory agency. These individuals were known to have frequent contact with the population of interest. I briefed them about the study in-person or by phone and asked for assistance identifying participants.

Efforts to recruit participants were also made via posting to the NPS Center for Homeland Defense and Security's (CHDS) alum network and reaching out to a scam survivors' website administrator. Further, I solicited participants during education events at which I presented in September and November of 2022. Recruitment efforts occurred through December 20, 2022.

2. Field Interview Participants

The recruitment efforts led to the identification of three study participants. The low enrollment rate in the study may have been due to its focus on potential criminality. According to one person who assisted in recruitment efforts, "When they know they've been mules, they are afraid of being prosecuted. Even though I tell them it's all confidential and no info will be passed on that's provided to the researcher" (Message from a government employee to researcher, December 2022).

All three participants who consented to in-person interviews were adult victims of romance scams. Two were female, and one was male. The male was from Ohio, while both females were from Minnesota. Though none had acted as a money mule, one participant stated, "it was going there for the second one" when asked if an offender had asked her to transfer money (Interview of PV2, September 2022).

In-person case number one was identified via my non-law enforcement network. The first participant, labeled PV1, contacted me via email in September 2022. PV1 stated she had recently been scammed and that it was a horrible experience. She also stated that she had been widowed for about a year. She expressed a desire to help with the study. I interviewed PV1 in a public location in September 2022.

In-person case two was identified via my law enforcement network. This second participant, labeled PV2, contacted the researcher via email in September 2022. PV2 stated she had been the victim of two “scams of this type” (PV2 email to researcher, September 2022). I interviewed PV2 in a public location in September 2022.

I identified in-person case three via my non-law enforcement network. This participant, labeled PV3, contacted me by phone in September 2022. PV3 stated he had recently been scammed via a romance scam. I interviewed PV3 by phone in October 2022.

3. Data Collection

Before beginning an interview, I read an IRB-approved introductory script to the participants. The script laid out the purpose of the research and explicitly warned of the possibility that participants might reveal criminal conduct during the interview. Participants were also reminded they could end the interview at any time. I then provided the participants with an IRB-approved consent form. I gave the form to PV1 and PV2 in person and emailed it to PV3 in advance of the interview. The signed consent forms were digitized and saved on a secure NPS server. The original consent forms were destroyed.

The interviews followed a semi-structured format. The IRB approved interview questions in advance. However, not all participants were asked precisely the same questions in the same order. All interviews were audio recorded. I also utilized Otter.ai transcription software in tandem with the recordings. Study participants were made aware that the interviews were being recorded. They were offered the opportunity to review a transcript before it was included in the study. All three participants declined to review their transcripts.

The first two interview questions were designed to confirm that the participant was suitable for inclusion in the study. As noted earlier, I confirmed suitability at this point to avoid collecting human subjects data before obtaining informed consent. All three participants indicated they had been victims of an online romance scam. They were thus included in the study.

After the interviews, I read a postscript. This script thanked the participants for their time and informed them that the final thesis would be publicly available. I included the materials I used in Appendix A.

4. Data Preparation

The transcription from Otter.ai was uploaded to NVivo, a program that researchers use “to organize, analyze and visualize their data, finding the patterns it contains,” according to the company’s website.¹²⁷ Next, I listened to the audio recording while reviewing the transcript to ensure fidelity. I anonymized the data and performed some initial coding during the transcription-checking process. I deleted the original recordings once I prepared the final transcripts. I began detailed coding of the interviews after I began coding the archival case data.

B. ARCHIVAL CASES

The selection of archival cases was convenient and purposeful, guided by my previous knowledge and initial research. As noted earlier, my “day job” is as a police officer whose duties include conducting criminal investigations into romance scams and money mules. I was aware of three closed criminal investigations involving witting money mules due to my participation in those investigations. The investigations involved the collection of text message communications between offenders and money mules. I was aware that text messages between the offender and other victims were also captured. My experience as an investigator combined with my initial research and review of the literature suggested studying how different individuals reacted to the same offender would offer important insights into how offenders introduce money mule behaviors in the context of

¹²⁷ “About NVivo,” NVivo, accessed December 22, 2022, <https://help-nv.qsrinternational.com/20/win/Content/about-nvivo/about-nvivo.htm>.

romance scams. These cases would also allow an analysis of why some romance scam victims become money mules and others do not, presuming it was found that not everyone agreed to transmit money. The cases, then, would adhere to Boeri and Lamonica's admonition in *The Routledge Handbook of Qualitative Criminology* that convenience sampling must not be "merely convenient for the researcher" but also "appropriate for the study goals."¹²⁸ The selected cases were appropriate for this study.

1. Data Preparation

The anonymized historical text messages were designated archival cases 1 through 3. The simple shorthand A1, A2, and A3 refer to these cases. The suspects in the archival cases were designated AS1 to AS3. Individual victims or money mules were labeled sequentially by case number (e.g., AV1.1 for the first victim in archival case one, AV1.2 for the second victim in archival case one, etc.).

An initial review of the data revealed that communications in case A3 were between a single offender and one other individual. The offenders in cases A1 and A2 had each communicated with multiple individuals. The original data set includes a total of 143,172 text messages. The earliest message was sent in November 2016. The last message was sent in December 2020 (see Table 2).

Table 2. Archival Cases

Case	First Text	Last Text	# Phone Numbers	# Received Texts	# Sent Texts	Sum
A1	January 2020	December 2020	75	16,968	34,259	51,227
A2	February 2018	February 2020	146	59,066	29,015	88,081
A3	November 2016	December 2016	1	1,798	2,066	3,864
TOTALS			222	77,832	65,340	143,172

The "# Phone Numbers" category excludes the offender's phone number.

¹²⁸ Miriam Boeri and Aukje K. Lamonica, "Collecting and Interpreting Qualitative Data," in *The Routledge Handbook of Qualitative Criminology*, ed. Heith Copes and J. Mitchell Miller (New York, NY: Routledge, 2015), 128.

2. Initial Case Inclusion and Coding

I treated each series of text message communications between an offender and another individual as a separate case. I excluded cases with fewer than 20 text messages because they contained insufficient content for meaningful analysis. This criterion left 44 cases in A1 and 47 cases in A2. I included cases AV1.1, AV2.1, and AV3 because I knew they contained communications between an offender and a money mule who was first a victim of a romance scam. This fact notwithstanding, cases AV1.1, AV2.1, and AV3 met other later-developed inclusion criteria.

A cursory review of the remaining cases in A1 revealed that offender AS1 appeared to be involved in schemes other than romance scams. For instance, AS1's conversation with AV1.13 appeared to be an advanced fee scheme involving erotic massage. AS1 wrote,

What kinda service rate do you want to discuss...You are at the right place with original Japanese Nuru oil...I take deposit to prevent traffic of bookings and avoids appointment disappointment. I dont take peoples money and not render good service. Your money is refundable if you cant make it or cancel the appointment, (AS1 to AV1.13, April 2020).

Similarly, AS1 sent another individual a message that appeared consistent with an advanced fee scheme based on winning a lottery.

This is to inform you that you have won a prize money of ninety thousands dollars {\$100,000.00 USD} on the on going Facebook Lottery Jackpot, All participant were selected through a computer random integrated system drawn in 15 million E-mail address on facebook.com.so are you ready to claim? (AS1 to AV1.43, May 2020)

To ensure that only romance scam cases were included in the study, I relied on Alam's definitions of intimacy, passion, and commitment to screen the cases.¹²⁹ I created initial codes based on these definitions and then applied the codes to the cases and removed cases that did not include at least one of these codes. I found that 26 cases in A1 contained one or more of these codes. The other 18 cases were excluded from the study.

All 47 cases in A2 contained one or more of these codes. Therefore, no cases were excluded from A2 using this criterion. Case A3 was also reviewed using these codes and

¹²⁹ Alam, "Three Essays on Socially Engineered Attacks," 193.

met the criteria for inclusion in the study. At this stage, 74 cases remained eligible for inclusion.

I selected cases AV1.9, AV2.1, AV2.2, AV2.3, AV2.9, AV2.10, and AV2.16 for initial coding. I initially set aside AV1.1 and AV3 to reduce bias. In my role as a police officer, I had previously closely analyzed these text messages, albeit for a different purpose. I first developed codes from other cases to reduce the chance I would prejudge the data in cases AV1.1 and AV3.

I coded the archival cases using NVivo qualitative data analysis software. The codes developed in an individual case were constantly compared to those in the other cases. As coding continued, themes began to emerge among the codes. These themes included swindling and behavior consistent with acting as a money mule.

The offenders' use of "scripts" was also noted at this phase. For this study, a script was defined as an identical or nearly identical message that an offender sent to two or more individuals containing two or more sentences. I identified scripts by searching for longer sections of text sent by the offender and then looking for the text's use in other victim conversations. This method identified eight scripts among the cases (see Appendix B).

3. Thematic Sampling

After completing the initial rounds of coding on the first seven cases, I compared the additional cases against these codes. I added new cases to the study until theoretical saturation was met (i.e., the inclusion of a case did not result in the generation of new codes). I purposefully sought cases that included themes related to money mule behavior. Overall, 22 archival cases were included in the study (see Table 3). While the study only included 10% of the individuals who communicated with the offenders, it captured 94% of all text messages found in the original data set.

The line of inquiry into the effect of scripts in romance scams was eventually dropped because it did not appear to contribute to answering the main questions posed in this thesis, the questions of how and why romance scam victims become money mules. However, cases included in the study because of the presence of scripts were not subsequently excluded since each of those cases contributed to code and theme

development unrelated to the use of scripts. For transparency purposes, Appendix B contains the list of scripts originally identified for further study and cross-references the cases where they appeared.

Table 3. Date Range and Number of Texts per Identified Victim/Mule

Label	First Text	Last Text	# Victim Texts	# Offender Texts	Sum
AV1.1	March 2020	December 2020	13,268	27,030	40,298
AV1.2	July 2020	November 2020	627	1519	2,146
AV1.3	May 2020	July 2020	466	904	1,370
AV1.4	September 2020	November 2020	423	910	1,333
AV1.5	April 2020	May 2020	287	518	805
AV1.6	June 2020	June 2020	186	406	592
AV1.7	November 2020	December 2020	216	299	515
AV1.8	June 2020	July 2020	124	323	447
AV1.9	April 2020	April 2020	127	284	411
AV1.21	May 2020	May 2020	44	56	100
AV2.1	August 2018	February 2020	48,886	24,409	73,295
AV2.2	June 2019	September 2019	3697	1087	4,784
AV2.3	September 2019	January 2020	1087	161	1,248
AV2.4	November 2019	December 2019	632	391	1,023
AV2.7	November 2019	November 2019	328	307	635
AV2.8	December 2019	February 2020	417	184	601
AV2.9	December 2019	December 2019	267	237	504
AV2.10	December 2018	January 2019	234	124	358
AV2.15	November 2019	November 2019	117	102	219
AV2.16	June 2018	July 2018	87	98	185
AV2.19	June 2018	June 2018	84	93	177
AV3	November 2016	December 2016	1,798	2,066	3,864
TOTALS			73,402	61,508	134,910

C. COMPARING INTERVIEWS AND ARCHIVAL CASES

This study included a total of 26 cases involving 25 victims. Most victims interacted with one persona in the study. PV2 was the exception because she was victimized twice, leading to the difference between the case and victim numbers. Seven different offenders were also identified. At least two offenders (AS1 and AS2) presented multiple male and female personas depending on the victim with whom they interacted. I anonymized the

persona names in case the offender used the identity of a third-party victim (i.e., identity theft). I should also note that it is impossible to be sure each offender was a single person. There is no reason multiple offenders could not use a persona in a conspiratorial manner. However, this is irrelevant from the victim's perspective since they were in contact with a single persona they perceived as genuine.

I compared the cases developed from interviews with those developed from historical text messages. The codes and themes between the case types were congruent. The codes and themes derived from archival and in-person sources were combined, refined, and aggregated into dimensions. As the codes were condensed and themes emerged, I consulted the literature on romance scams and gullibility to aid in developing theoretical insights. This engagement informed the naming of certain codes. Specifically, the code "persuading" was influenced by Whitty's *The Scammers Persuasive Techniques Model*, and the theme "inducing gullibility" emerged from readings in *The Social Psychology of Gullibility*, which was edited by Joseph Forgas and Roy Baumeister.¹³⁰ Likewise, the term "emotional loneliness" was taken from Buecker et al.'s article *Loneliness and the Big Five Personality Traits: A Meta-Analysis*.¹³¹

Ultimately, 161 offender codes and 100 victim codes were consolidated into 18 codes, six themes, and two aggregate dimensions for the offenders, and 21 codes, six themes, and two aggregate dimensions for the victims/money mules. I organized this data into a data structure to aid in visualization and theory building consistent with Gioia's approach to reporting on qualitative research (see Figure 3).¹³²

¹³⁰ Whitty, "The Scammers Persuasive Techniques Model"; Joseph P. Forgas and Roy F. Baumeister, eds., *The Social Psychology of Gullibility: Fake News, Conspiracy Theories and Irrational Beliefs* (New York, NY: Routledge, 2019).

¹³¹ Susanne Buecker et al., "Loneliness and the Big Five Personality Traits: A Meta-Analysis," *European Journal of Personality* 34, no. 1 (January 2020): 8–9, <https://doi.org/10.1002/per.2229>.

¹³² Denny Gioia, "A Systematic Methodology for Doing Qualitative Research," *The Journal of Applied Behavioral Science* 57, no. 1 (March 2021): 26, <https://doi.org/10.1177/0021886320982715>.

I also constructed data tables demonstrating quotes that were used to support code formation for cases AV1.1, AV2.1, and AV3. These data tables are included in chapters III and IV. The quotes in the tables serve as the “characteristic examples of data” that Glaser and Strauss called for in their seminal work.¹³³ Additionally, Table 13 in Appendix D shows the estimated length of the relationship that existed between the offenders and these three individuals.

Actual text messages appear in the data tables and the chapters just as the victims and offenders wrote them, with grammatical and stylistic errors intact. Data tables for the remaining 23 cases only indicate whether a code was or was not located in the case due to the volume of analyzed data. However, direct quotes are included in the Offender Communication and Victim and Money Mule Communication chapters (see Appendix D).

¹³³ Glaser and Strauss, *The Discovery of Grounded Theory*, 5.

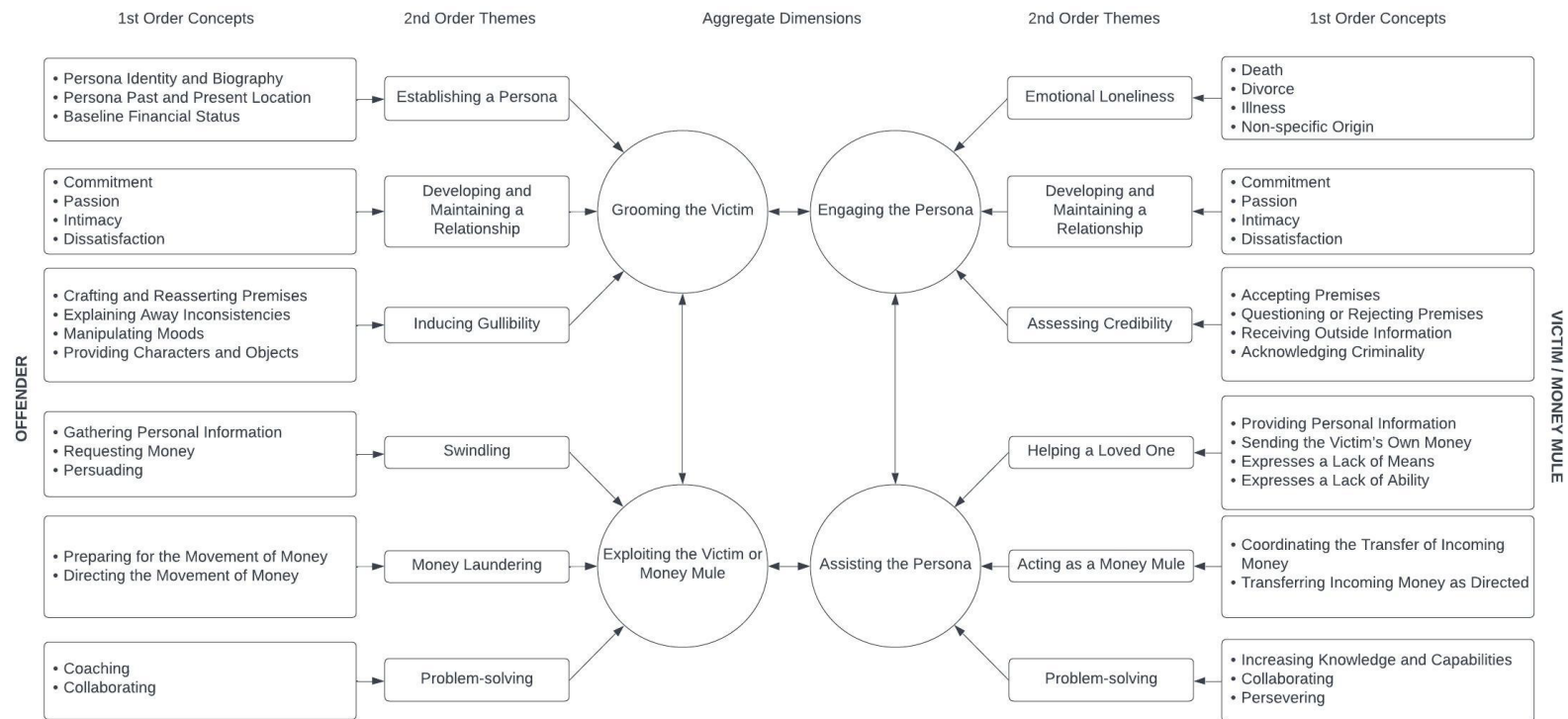


Figure 3. Data Structure

III. ANALYSIS OF OFFENDER COMMUNICATION

Although I developed the codes by examining offender-victim interactions, I present the analysis of offender and victim cases independently. In this chapter, I examine how the offenders' language supports their goals and present data tables to support my findings. This level of detail is provided to substantiate the coding schema and illustrate the distinctions between codes.

My analysis shows that the exploitation in romance scams is predicated on the offender's expression of romantic language and repetition of scheme-relevant premises via a persona. This finding is consistent with grooming as described in previous romance scam studies. However, my analysis also shows that the offender uses the romance scam as a basis to gain victim compliance with requests to transfer incoming money (i.e., act as a money mule). This finding allows me to elaborate on concepts related to grooming and gullibility to encompass victims who become co-offenders.

A. GROOMING THE VICTIM

My analysis of the archival cases and interviews suggests that offenders carefully introduce and repeat premises that justify later requests for money from the victim. In prior studies of romance scams, researchers refer to the process of transforming a person from an online relationship seeker to a victim as "grooming."¹⁴⁰ This study finds that the offender begins the grooming process by creating and animating a persona. Next, the offender develops the relationship by expressing love, faithfulness, affection, trust, and sometimes even anger toward the victim. Finally, via repeated assertions and storytelling, the offender presents a series of false premises to a victim. The offender appears to strategically design these false premises to induce gullible responses to future exploitative requests. The offender accomplishes this by manipulating emotions and relational norms and taking advantage of the victim's decision-making errors. In addition to the quotes listed in each section, Tables 4 through 6 contain several quotes supporting these findings.

¹⁴⁰ Whitty, "Anatomy of the Online Dating Romance Scam," 444, 450; Cross, Dragiewicz, and Richards, "Understanding Romance Fraud," 1306; Whitty, "The Scammers Persuasive Techniques Model," 676–81; Alam, "Three Essays on Socially Engineered Attacks," 73.

1. Establishing a Persona

Because the online romance scam depends on a relationship, the offender had to create a persona with which the victim interacted. To create the persona, the offender presented numerous false premises. These included the offender's name, location, financial status, and biographical facts. Elements of this theme were found in all 26 cases examined. The offender uses the established persona throughout the entirety of the scheme. In addition to the in-text quotes, Table 4 provides additional quotes between offenders and the three money mules in the study.

Table 4. Quotes Supporting Codes under the “Establishing a Persona” Theme

2nd Order Themes	1st Order Codes	Label	Quotes Supporting Code
Establishing a Persona	<i>Persona Identity and Biography</i>	AS1	“You have all my information, you have my ssn, you have my ID” (To AV1.1, May 2020).
		AS2	“I’m always a one woman man ...after the death of my ex” (To AV2.1, July 2018).
		AS3	“It’s [AS3], all my numbers and phone are misbehaving” (To AV3, November 2016).
	<i>Persona Past and Present Location</i>	AS1	“Are you going to drive to Canada and pick me up” (To AV1.1, July 2020).
		AS2	“At kunar where I told you” (To AV2.1, January 2020).
		AS3	“It’s cold now in Dubai” (To AV3, November 2016).
	<i>Baseline Financial Status</i>	AS1	“you know that my management is still owing \$12million” (To AV1.1, August 2020).
		AS2	“Am a Us Army Airborne...I fly the copter and sometimes inspect and fix trucks” (To AV2.1, January 2019).
		AS3	“very beginning he told me he hide only the one and a half million. Then later he told me I hide another 1 million” (Transcript of Police Interview of AV3, August 2017).

a. *Persona Identity and Biography*

The most basic element of the persona was the name used. Along with a name, the offender provided photos that they asserted to be of themselves. The offender frequently enriched the background story of the persona with additional details such as family history.

As an example, after one suspect provided a victim with a name and birthdate, the suspect went on to state, “I am the only child of my parents. I lost my parents late last year, I really do not have a big family as such” (AS1 to AV1.4, September 2020).

I found the offender sometimes used identity theft in creation of the persona. Identity included the offender presenting a different romance scam victim’s identity as their own. For example, a victim inquired of an offender “What is your full name?” (AV2.8 to AS2, December 2019). The suspect replied by providing the actual identity of AV2.1. Thus, the offender assumed the identity of a different romance scam victim to facilitate grooming of a second victim.

The offender also used this time to establish the persona’s personality. For instance, one suspect wrote, “I’m basically a very positive person who also loves humor and laughter and would like someone with an adventurous spirit and a positive attitude who can see the funny side of life, someone who is open and willing to learn new things” (AS2 to AV2.9, December 2019). In another instance, the same suspect asserted “I love to serve my country” (AS2 to AV2.10, January 2019).

The offender frequently mirrored the victim’s assertions at this phase in a likely effort to appear similar to the victim. For instance, a suspect sent a script to three different victims that exhibited how the offender can mimic a victim’s statement, describe the persona, and express future desires in one communication. The suspect wrote,

I think we are Looking for the same things but mine in a Woman, Just that i am Looking for a nice, Honest, Kind and Caring Woman, a Woman that will Love and be with me for the Rest of my Life....Am not looking for someone to date but someone to spend the rest of my life with, All i need from you is just being sincere to me, make me feel secured, appreciate, love, care and being understanding, All my life has been engulfed with misery and loneliness,i watch my life layed wide spread in front of me and didn’t know what to do with it, my life has been so boring and hope with someone who is ready to Love me for who i am now it’s gonna change for the best (AS2 to AV2.4, June 2019; AS2 to AV2.15 and AV2.16, November 2019).

The offender relied on these basic persona details throughout the scam. Offenders’ use of persona identity and biography was present in all cases examined.

b. Baseline Financial Status

Conversations about money frequently occurred throughout the scheme. In fact, the word “money” itself is present in 24 cases and appears 3,806 times. The offender frequently predicated these money conversations on assertions the offender made about the persona’s financial status and source of income, like employment. The code baseline financial status was used to capture references to the persona’s purported “steady state.” As such, the code does not include emergent, alleged needs for money or immediate opportunities to get money. The code did include references to the persona’s foreseeable opportunities to gain wealth.

Military employment was the declared occupation for the persona on several occasions. For instance, a suspect told a victim, “Am a Us Army Airborne...I fly the copter and sometimes inspect and fix trucks” (AS2 to AV2.10, January 2019). Likewise, the same suspect claimed in a message to a different victim, “Am an E18 Sergeant which means a special force sergeant am not supposed to tell you my MOS but I trust you with it ok” (AS2 to AV2.7, November 2019). Military service appeared to provide later explanations for the offender being unable to meet the victim and to support the offender’s later requests for money.

Low-wage jobs were sometimes the purported employment. A suspect told a victim, “I work as a cashier” (AS1 to AV1.7, November 2020). The same suspect informed a different victim “im a female fashion designer, i design and make female wears, bikinis and lingerings” (AS1 to AV1.2, July 2020). This suspect even claimed unemployment by asserting “have not been working because of the covid 19 pandemic” (AS1 to AV1.3, May 2020). This lack of income was later used as a context for requests for money.

Conversely, the offenders sometimes claimed to have wealth, property, or good-paying jobs. One suspect claimed, “I own my home in Kentucky” (AS2 to AV2.15, November 2019). A victim I interviewed stated that one suspect asserted his “inheritance is \$12 million dollars” (Interview of PV2, September 2022). Another suspect texted a victim, “Am in a big mess with my inheritance I was trying to keep that from you but I think it’s time I let you know honey” (AS2 to AV2.1, March 2019). The word “inheritance” appeared in 12 of the cases. Like a lack of income, inheritance was used as a pretext to ask

for money in a manner consistent with an advanced fee scheme. In other words, the offender would claim to need money immediately to access future wealth.

c. Persona Past and Present Location

The offender also made assertions regarding the persona's location. Like personal identity and biography, persona past and present location appeared in all cases. It included the persona's current location as well as past residences. The offenders often made these assertions as simple statements, such as one suspect declaring, "I live in Cleveland ohio" (AS1 to AV1.8, June 2020). These alleged locations seemed to hold significance both to the victims and the direction the scam took. For instance, one suspect claimed he was located in Rochester, Minnesota. The victim stated this was important to her because "it was like drivable. I knew the town really well," and the town was "90 minutes, an hour, from here. And being able to actually physically get together was reasonable, because it wasn't very far" (Interview of PV2, September 2022).

Other times, the offender claimed to be in more distant locations. A suspect, for example, told a victim he was in Fontana, California while the victim was in Minnesota (Interview of PV1, September 2022). The offender could then use the distance as an excuse for the fact they could not meet. For example, a suspect messaged a victim, "I moved out of Tn i was being used by friends and my ex ,I had to move in with my college here in Minnesota am sorry" (AS2 to AV2.9, December 2019). The offender followed this message with the assertion, "that was why I wanted a distance relationship so we get to know more about each other before meeting and jumping into bed" (AS2 to AV2.9, December 2019).

The offenders sometimes relied on physical distance to explain other questionable behaviors. For example, a victim who had not heard from the persona for a while asked, "Are you stuck in Kabul? How come you don't answer me?" (AV2.1 to AS2, January 2020). The offender replied, "Okay honey. Am still stuck babe" (AS2 to AV2.1, January 2020). Thus, the persona's purported location served several functions for the offender.

2. Developing and Maintaining a Relationship

Creating a romantic relationship between a persona and a victim to defraud the victim essentially defines a romance scam. Therefore, only cases that included language related to forming and maintaining a romantic relationship were included in this study. I relied on prior research by Md Nabid Alam at the University of North Carolina at Greensboro to form three out of the initial four codes under this theme and the identically named theme under the victim and money mule heading. This theme captures expressions of positive and negative emotions associated with forming and continuing long-term, intimate relationships. The offender later relied on the resultant relationship when making exploitive requests of the victim. Table 5 offers additional quotes related to this theme.

Table 5. Quotes Supporting Code Formation under the “Developing and Maintaining a Relationship” Theme

2nd Order Themes	1st Order Codes	Label	Quotes Supporting Code
Developing and Maintaining a Relationship	<i>Commitment</i>	AS1	“Cause i wanna be with you and spend my entire life with you” (To AV1.1, August 2020).
		AS2	“I HAVE CHOOSE TO LOVE YOU TILL DEATH DO U.S. APART” (To AV2.1, November 2018).
		AS3	“I love you forever baby” (To AV3, November 2016).
	<i>Passion</i>	AS1	“I want to romance and make love with you all night” (To AV1.1, April 2020).
		AS2	“You want sex honey?” (To AV2.1, January 2019).
		AS3	“make love on the couch” (To AV3, November 2016).
	<i>Intimacy</i>	AS1	“You are the first the first person I wake thinking about you this morning and I wanna let you know that I love you so much and I cherish you a lot” (To AV1.1, April 2020).
		AS2	“I love you babe and you’re always in my thought” (To AV2.1, March 2019).
		AS3	“I just wanted you to know how much I truly do care. You’re always in my thoughts” (To AV3, November 2016).
	<i>Dissatisfaction</i>	AS1	“I guess you must be cheating on me and still lying to me” (To AV1.1, August 2020).
		AS2	“Honey all this words saddens my heart” (To AV2.1, March 2019).
		AS3	“I get sad when you talk this way” (To AV3, November 2016).

a. Commitment

I used Alam's definition of commitment to code for this dimension of the scam. Alam wrote, "commitment in a relationship refers to whether there is understanding about the future and whether the partners see each other together in the long run."¹⁴¹ Offenders used language of commitment fitting this definition in all except one of the cases.

The offenders commonly made assertions they would be with the victim for life. One suspect claimed, "I will be with you and grow old with you and I will never leave your side" (AS1 to AV1.3, May 2020). The same offender told a different victim, "I want to spend the rest of my life with you" (AS1 to AV1.5, April 2020). A different offender texted a victim, "You are mine forever baby" (AS3 to AV3, November 2016).

Offenders often used terms associated with marriage to convey commitment. For example, one suspect texted, "I want you to be my wife honey" (AS1 to AV1.9, April 2020). A victim I interviewed reported a suspect discussed a wedding with her including that "I've designed your ring. We're gonna get married in Ibiza" (Interview of PV2, September 2022). One relationship went so far as the victim and suspect imagining a future child together, which they named Lisa. The offender messaged, "I want to be with you, live with you and see our children's children." The offender followed that text with, "Baby i can't wait to have the ring on my fingers and i cant wait for people to start calling me mrs [AV1.1]." Finally, the offender asserted, "I got alot of plans for you, for [AV1.1's son] and for our daughter Lisa and our family" (AS1 to AV1.1, August 2020).

Similarly, a suspect told a victim, "I want us to be the best family and we can enlighten the kids more about everything" (AS2 to AV2.1, May 2019). The same suspect also assured a different victim, "I promise to stay with you through the thick and thin" (AS2 to AV2.19, June 2018). Likewise, a suspect reportedly asserted to a victim, "I want to grow old with you" (Interview of PV1, September 2022). A victim reported the suspect "would be talking about you know, getting a house with a couple of dogs" (Interview of PV3, October 2022). Through these assertions, offenders painted a picture of a committed life together with the victim.

¹⁴¹ Alam, "Three Essays on Socially Engineered Attacks," 193.

b. Passion

Here, too, Alam's research provided a useful definition. According to his research, "passion in a relationship is an intense feeling of love, affection, and desire."¹⁴² The desire dimension in this study included expressions of attraction based on a recipient's observations of photos that were texted or the statements of interview participants. For the sake of decorum, explicit descriptions of sex acts were not cited as examples for the passion code, though they were present in many of the cases. Examples of language associated with passion were found in all except two cases.

The offenders frequently averred in text messages that they found the victim attractive. For instance, an offender texted "dont forget you are a sexy man" (AS1 to AV1.2, July 2020). The same offender texted a different victim, "I cant stop looking at your pictures, you cute smile and cute beards I love you so much" (AS1 to AV1.8, June 2020).

Physical passion was approximated through the exchange of explicit sexual messages commonly known as "sexting." It also appeared there were sometimes exchanges of photos and videos. As an example, an offender inquired, "Babe we can make love tonight and I will make video for you my love" (AS1 to AV1.5, April 2020). PV2 likewise reported PS2.1 was "Always very romantic and sending photos."

The messages coded as passion clearly portrayed the idea that the persona desired the victim. In an ironic statement given its relation to a romance scam, one offender wrote "I want to steal your heart" (AS2 to AV2.10, December 2018). Another offender conveyed a sense of desire by texting, "I am so excited to have you as my lover ??" (AS 3 to AV3, November 2016). Meanwhile, a different offender asserted, "You are my true love. I've been searching for you. I finally found my soulmate" (Interview of PV1, September 2022).

Scripts containing passionate language also surfaced in the texts. In one example, an offender sent the message, "I never thought of falling in love with someone I barely knew. Then suddenly I met you one day and something in my ear whispered that this is the

¹⁴² Alam, 193.

girl that I have ever wanted in my life” to four different victims (AS 2 to AV2.1, AV2.4, AV2.7, and AV2.15, November 2019).

c. Intimacy

The definition of the code for intimacy was also adopted from Alam’s research. Alam defined intimacy as “a feeling of being close, emotionally connected, and supported. It also means regular and meaningful communications.”¹⁴³ Intimacy also included apologies and efforts to restore closeness following arguments and disagreements between the persona and victim. I coded expressions of intimacy by the offender in all 26 cases in this study.

Intimacy appeared primarily in two forms. On the one hand, offenders made one-off expressions of love, concern, and connection. An example is, “How is your day going?” (AS2 to AV2.16, June 2018). Similarly, the same offender wrote, “I can’t wait to show you how much I love you. The little things I do all through the day for you are not enough to let you know that you mean the world to me. The most pleasing thing I have ever seen is your smile. Keep smiling for me, baby. Enjoy this brand new day that nature has given us” (AS2 to AV2.2, June 2019).

Sometimes the concern even seemed counterproductive for the offender such as when one offender warned that, “any one asking to buy gift cards and send money is a scam” and “i dont want you to get hurt” (AS1 to AV1.2, July 2020). The offender concluded by advising the victim he should tell another person he had met online “to take a picture to give you a peace sign” (AS1 to AV1.2, July 2020). These messages give the impression the persona genuinely cared for the victim’s welfare.

On the other hand, some of the cases contained evidence of what appeared to be the sharing of daily experiences by the victim with the offender. Take, for example, this exchange between a victim and an offender:

Victim:	On way to the race track.
Offender:	Hold on if they ask another question i will let you know
Offender:	Do you have race track today honey
Victim:	Yes baby.

¹⁴³ Alam, 193.

Offender: Who is going with you honey
Offender: What about [victim's son]
Victim: My friend the driver of the car his wife and me dad and
[victim's son]
Offender: Wow
Offender: I wish im there with you honeu
Offender: My regards to dad, your friend and his wife (AS1 and AV1.1,
August 2020)

This daily, close communication wove interaction with the offender into the fabric of the victim's life, building a dependency on future communication.

Although this type of communication appeared to reflect a growing or maturing relationship from the victim's perspective, the offender could use it to further the scheme by improving their knowledge of the victim. One victim noted of her conversations with the persona, "So we communicated for months. And he got to know a lot about me" (Interview of PV2, September 2022). Thus, this growing closeness between victim and persona became a vulnerability for the victim that the offender could later exploit.

d. Dissatisfaction

Dissatisfaction with the relationship was observed in this study's data, unlike Alam's study. Dissatisfaction captured the expression of negative emotions such as disappointment, gaslighting, and not fulfilling obligations within the context of an intimate relationship. Conversations that included dissatisfaction occurred quite often in the archival text messages and were also referenced during the in-person interviews. Dissatisfaction was less prevalent than other codes included under the relationship theme. It appeared in 15 of the 26 cases.

Some of the expressions of dissatisfaction were simple and straightforward. For example, an offender texted, "You are pissing me off why are making me feel like that?" (AS1 to AV1.1, April 2020). The offender messaged a different victim, "I hope you won't hurt me again by leaving me" (AS1 to AV1.2, July 2020). Similarly, an offender confronted a victim with, "What's the problem now ? Why will you believe a stranger I don't even know over me ? That's not good !" (AS2 to AV2.2, June 2019).

In some instances, the offender seemed willing to end the relationship. For example, an offender texted a victim, “Am not in for your mind games and lies so you can just go and never text me again you lied so much already” (AS2 to AV2.2, July 2019). The same offender messaged a different victim, “LEAVE ME THE F ALONE” (AS2 to AV2.3, September 2019).

Disappointment mixed with guilt and ascribed to a victim’s action, sometimes referred to as “gaslighting,” occasionally surfaced in the messages. For instance, an offender texted “This is the period I always feel like doing something stupid to myself” (AS3 to AV3, December 2019). The offender followed that message with, “The only person in the world helping me now is tired of me, how can I not want to kill Myself” (AS3 to AV3, December 2019).

3. Inducing Gullibility

This theme covers offenders’ use of techniques intended to induce victims to accept false premises through repetition, referential objects, or by providing narratives intended to be mentally processed easily by the victim. The offender used storytelling to deliver the premises. When a victim confronted an offender or rejected a particular assertion, the offender sometimes provided explanations based on previous premises or introduced new storylines. Additionally, the offender frequently included various characters, documents, and objects in the tale. Occasionally, the victim could interact with some of these characters or objects. This interaction could include phone calls from the offender’s co-conspirators, who were playing a role, or the employment of websites designed to bolster an offender’s claims. Additional quotes for this theme are displayed in Table 6.

Table 6. Quotes Supporting Codes under the “Inducing Gullibility” Theme

2nd Order Themes	1st Order Codes	Label	Quotes Supporting Code
Inducing Gullibility	<i>Crafting and Reasserting Premises</i>	AS1	“Because you know about the inheritance and you know for a long time that my bank will send money to your account I told you this before” (To AV1.1, May 2020).
		AS2	“I told you about the shares my dad had with a foreign country right?” (AV2.1, March 2019).
		AS3	“Oh baby, you know I am doing all this so I don’t have to ask you for money and also pay all my bills and leave here” (To AV3, November 2016).
	<i>Explaining Away Inconsistencies</i>	AS1	“Baby everything is real” (To AV1.1, August 2020).
		AS2	“They would say scam because it’s another country” (To AV2.1, May 2019).
		AS3	“I am really sorry and I am not into money laundering” (To AV3, December 2016).
	<i>Manipulating Moods</i>	AS1	“Babe I wanna be with for cabin and I will make sure I do everything possible for me to make to home with you okay” (To AV1.1, June 2020).
		AS2	“I got a text that [son] is so happy and has been in his room with his friends and they been having nice time (To AV2.1, November 2018).
		AS3	“I really need to be with you this xmas” (To AV3, November 2016).
	<i>Providing Characters and Objects</i>	AS1	“My lawyer need those information for them to make some payment” (To AV1.1, May 2020).
		AS2	“What do I tell [son] and Nana?” (To AV2.1, September 2018).
		AS3	“I am sorry, the clients are replying me really late” (To AV3, November 2016).

a. Crafting and Reasserting Premises

After establishing the persona and while building the relationship, the offender presented a series of premises. These stories added a fuller backdrop to explain delays in meeting in person, requests for money, or difficulties with communication. These were frequently long-term stories that could last the life of the scheme once introduced. Premises were repeated often and frequently built on one another in an attempt by the offender to tell a coherent tale. These stories were used to add life, drama, and explain later requests for money. Crafting and reasserting premises was observed in all 26 cases.

The stories were sometimes used to explain otherwise suspicious behavior, such as a lack of communication. For example, one offender claimed, “My cell is not a good one, i will also like to hear your voice too but i will get a new phone soon and i will give you a call immediately i get a new phone” (AS1 to AV1.4, September 2020). Another time, an offender stated, “I have to pay for minutes on my cell to talk to you” (AS1 to AV1.3, May 2020). This offender explained, “Cost me \$100 to prepaid my phone, I can call, text and send you unlimited video and pictures” (AS1 to AV1.3, May 2020). The offender concludes by explaining the inability to pay for the phone by adding, “I dont mean to bother, I have spend all my money at the court that is why” (AS1 to AV1.3, May 2020).

The offender’s stories often relied on previously established characteristics of the persona. For example, an offender built on a previous assertion regarding an inheritance when texting a victim, “I told you about the shares my dad had with a foreign country right ?” (AS2 to AV2.1, March 2019). Likewise, the offender relied on a mix of a previous premise regarding his location and current events when asking the victim, “Did you see all that is going on in the news ?” and then adding “I can’t travel back to Kabul as I have to be careful here” (AS2 to AV2.1, January 2020).

Once told, premises were reiterated often. For instance, an offender elaborated, “It’s locked down to tax agencies but nana and my son lives at Ar ...I told you that before,” when discussing a home the offender claimed to own in Kentucky (AS2 to AS2.10, January 2019). Similarly, an offender asserted “I told you about my brands” (AS1 to AV1.6, June 2020). The offender followed that message with, “Babe I thought I told you this before honey, we have discussed about not more then 3 time this is the 4th time we are talking about this, i ask you to be patient and you promise you be patient and you gonna work hand in hand with to achieve my dream and we can be together my love” (AS1 to AV1.6, June 2020). Thus, repetition plays an important role in the presentation of premises.

Many times, the premises involved alleged movement from the persona’s originally established location to another. This switch sometimes happened via an assertion that the persona was coming to meet the victim as when a victim texted, “I’m coming home on Thursday or friday honey” (AS1 to AV1.1, August 2020). Other times, the persona claimed to be going to a more distant location. For example, a victim stated a persona told her,

“after like 20 days he told me he’d went to Dubai” (Interview of PV1, September 2022). Similarly, a victim stated that “before he came home from Florida, he had he flew a private jet to Lodz, Poland” when discussing a persona she had a relationship with (Interview of PV2, September 2022). The movement itself or the new location often later served as the backdrop for an exploitive request.

The stories quite often established a need for money either because of an emergency or a current inability to obtain cash. This offender message illustrates this concept, “Mom is seriously in need of the money for her surgery and my lawyer is so concerned, money, he thought may be i screwed all the money or may be we dont wanna take care of mom” (AS1 to AV1.1, August 2020). The latter concept is evident in the same victim’s text to a different victim, “Baby alot of my customers are owing me and because of the pandemic of CORONAVIRUS that is why im not getting orders” (AS1 to AV1.2, July 2020). Both approaches provided the backdrop to ask the victim for money to assist with the persona’s need.

b. Explaining Away Inconsistencies

Often the victim did not fully believe or accept a story as asserted by the offender. The offender frequently then provided additional context in the form of reasons or excuses. The stories could build on past premises or general understandings of how societies operate (e.g., difficulty interacting with government bureaucracies). Explaining away inconsistencies was recorded in 25 of the 26 cases.

Many times, the offender offered only vague reassurance to allay the victim’s fears. For instance, one offender responded to a victim’s fears with a simple, “Im not lying” and later, “Im not playing you babe” (AS1 to AV1.1, July 2020). A victim’s willingness to accept such flimsy denials may indicate the presence of confirmation bias (i.e., a person’s tendency to easily believe “facts” that conform to their prior beliefs). An example is this victim who relayed to the offender that she had told her therapist about him:

Victim: He said people like you use lonely woman to get money

Victim: And that I should stop talking to you

Offender: Then his really out of his mind ! :rage::rage::rage::rage:

Victim: I didn't say a lot either I just told him I how we met and how comfortable you make me feel

Offender: How will he just sit comfortably and start talking about someone he doesn't know

Offender: His a pussy ass !

Victim: Some thrypist become them because they themselves are messed up

Victim: I'm not going back to him (AV2.1 and AS2, September 2018).

When the offender provided a deeper explanation, they often wove a past premise into the excuse. In answer to a victim questioning why an offender needed to know whether she had a credit card, the offender texted, "Because am an 18B special force and a team leader so the Mg from FortKnox wants to give me payment for me and my team mates but as the leader i have to be the one to get the money from them" (AS2 to AV2.16, June 2018). This offender further explained, "To make the payments for the rest team mates and i will need a credit card to receive the payment" (AS2 to AV2.16, June 2018). Similarly, an offender responded to a victim's request for more identifying information by relying on an earlier claim of military service. The offender messaged, "I have all of those but I can't for security reasons ! Even your cousin wouldn't share that with anybody" (AS2 to AV2.2, June 2019).

Sometimes the offender appeared to rely on the expectation of trust in a relationship to form the excuse. An example is an offender writing, "Why could you believe what you see from google and what you hear from other people" (AS1 to AV1.2, November 2020). Ironically, the offender then told the victim, "Don't believe anyone or the internet" (AS1 to AV1.2, November 2020). Another example is an offender asserting, "Listen you need to trust me" (AS1 to AV1.6, June 2020).

The offender sometimes tried to lead the victim into deceiving themselves, as seen when a victim reported that an offender asked her, "why would I spend all this time making a profile and doing all this work if I'm not real?" (Interview of PV1, September 2022). Offenders added entirely new details, as illustrated by a victim's statement that "I did ask her why she has a thick accent. She goes 'well, I, you know, I was raised over here in

England.’ And I go, ‘what about your brother?’ ‘Well, he was raised over here too.’” (Interview of PV3, October 2022).

c. Manipulating Moods

The offender sometimes concocted stories that purportedly happened to the persona that were intended to produce a positive or negative emotional response from the victim. These were generally short-term stories that were less intricate than those coded as “Crafting and Retelling Stories.” It differs from text coded as persuading in that, with manipulating moods, language is motivating only in the context of the specific relationship. It stands apart from dissatisfaction because the topic regards something outside the relationship, whereas dissatisfaction addresses something about the relationship itself. Manipulating moods stories could eventually be incorporated into long-term stories if they were retold. Manipulating moods appears in all but two of the cases.

Throughout the cases studied, offenders often promised to meet. The victims replied with language indicating they were happy or excited at the development. When the meeting failed to occur, a request for money often followed. The following text from an offender illustrates the point, “I have a suggestion honey ..will you be able to pay for my way to go deliver this jewelries I made ? So I can have more money to come down to you or I forget about them and you pay for my way to you babe ?? Let me know what you think when you get my text” (AS2 to AV2.9, December 2019). Similarly, an offender used the story of a failed meeting to motivate a victim to send money. The offender wrote, “I have unpacked the luggage ... I will stay back if you want me to stay back at home ... You and i have been waiting for the day i will come home ... I love you” (AS1 to AV1.1, July 2020). One victim I interviewed noted that the offender “would have a circle around the last destination in green and then there would be an arrow to it and I can’t wait to see you!” (Interview of PV1, September 2022).

The offenders also used language designed to raise concerns in the victim regarding the persona’s welfare. For example, an offender texted, “I use all the money i have for the trip yesterday i didn’t have a single water drink all through yesterday got home late and wake up early this morning woring on paperwork and now on a cue to get s stamp” (AS1 to AV1.1, July 2020). The same offender sent a different victim, “My refrigerator is empty”

followed by “I dont have anything to eat at home, I’m just stranded right here” (AS1 to AV1.8, June 2020).

The following conversation shows how an offender weaved welfare concerns into the dialogue to premise a prior or future request for money.

Offender: You mean I tell lies ?
Victim: I love you
Offender: You love me really ?
Victim: Yes i really do but i should be asking you do you love me i
dont want to fight with you anymore
Offender: You love me but watch me starve (AS2 to AV2.2, June 2019).

Additionally, the offender sometimes introduced an emergency that carried significance due to the relationship between the persona and victim. For instance, an offender texted, “My mom is dying” (AS1 to AV1.1, August 2020). This text preceded a request for money. The offenders also manipulated moods to encourage the victim to be more isolated. This is shown in an offender’s message to a victim, “Do you promise to stop talking to him and any other person you’re talking to? Am scared of being hurt as am not talking to anyone else but you” (AS2 to AV2.15, November 2019).

d. Providing Characters and Objects

The offenders frequently wove other characters into the premises they offered. The characters explained delays, suspicious behaviors, or requests for money. Sometimes, the victims interacted with an offender’s co-conspirators who had adopted these roles. In addition to introducing other people into a scheme, offenders sometimes sent documents, referred victims to websites, or sent physical gifts to the victim. These acts added depth to the premises on which the offender based the scam and acted as another repetition of the premises. Characters or objects were mentioned in all but one case that was studied.

Family members were frequently introduced characters. An offender texted, “[son] was requesting for an amazon gift card for his PlayStation today” (AS2 to AV2.19, June 2018). Similarly, an offender told a victim, “My dad was a traveler he never had time for the family his always concerned about his work and his attorney.. he would choose his attorney over any of the family members” (AS2 to AV2.15, November 2019). One victim

reported that while being scammed by an offender, “he did have his daughter calling once” (Interview of PV2, September 2022). She went on to explain, “When she called me one night to tell me that she had been trying to get money for her dad. It was all... they were working this together trying to get money for her dad. And she’d gone to an old family friend, and he molested her, and but she couldn’t tell her dad that and I was like, ‘wow, that’s terrible.’” (Interview of PV2, September 2022).

Offenders frequently referred to lawyers. For example, an offender texted a victim, “My attorney will like to meet you,” and “He call you tomorrow” (AS1 to AV1.1, June 2020). This offender also mentioned a lawyer to a different victim. The offender claimed, “I have to go see my attorney today I have a meeting with him and when I come back I will do chores and laundry” (AS1 to AV1.3, May 2020).

Like family members, lawyers were not always just introduced in concept. Sometimes a victim interacted with a person claiming to be the persona’s lawyer. One victim texted an offender that “I talked to your lawyer honey,” and “Your lawyer was very understanding.” The offender, replied, “Yes i know you talk to my lawyer” (AS1 to AV1.1, August 2020). A victim I interviewed also reported that, while being scammed by an offender, “the attorney or ‘attorney’ reached out several times just with a request for that information” (Interview of PV2, September 2022).

Offenders also used websites to bolster their claims. One offender messaged, “I wanna show you something [https://\[website\]](https://[website]) Username:[username] Password: [password] Amount :\$6,000,000,” and “Login to the account” (AS1 told AV1.2, July 2020). A victim related a similar experience when she reported, “He also sent me a link to a supposed Barclays Bank account where he gave me a password and I can go in and look at the money that was in this account and it really looked fairly legit” (Interview of PV2, September 2022).

Offenders used other referential means to increase credibility. One victim reported being shown “a document that looks real” (Interview of PV1, September 2022). The victim also reported receiving a package from the persona that contained “two gowns.” The victim went on to explain that the persona reported hiding jewelry in the hem of one of the gowns. The persona instructed her to “take the hem out of the sleeve.” When the victim did so, she

reported, “lo and behold there it was...this necklace...and this ring” (Interview of PV1, September 2022). Another victim reported the offender “sent a gift from Amazon to my sister for her birthday” (Interview of PV2, September 2022).

B. EXPLOITING THE VICTIM OR MONEY MULE

After an offender sufficiently groomed a victim, the offender made exploitative requests. The offender used individuals for financial gain, to aid in money laundering, or both. However, the beginning of exploitation did not indicate the end of grooming. Throughout the entire scheme, the offender maintained the relationship and created and defended premises. This continued grooming activity appeared to increase some victims’ compliance with exploitative requests.

Offenders also took advantage of victims by using them as money mules. After introducing the appropriate premises needed to justify the movement of money through the victim’s account, the offender began to provide information about money that would be coming to the money mule. Once the money mule received the money, the offender directed how the money mule should transfer the money and to whom. Occasionally, the victim or money mules encountered difficulties transferring either their own money or money they received from another person. In those cases, the offenders sometimes problem-solved with the victim or money mule by coaching or collaborating with them.

1. Swindling

The “swindling” theme encompasses the offenders’ attempts to obtain something valuable from the victim and subsequent efforts to persuade reluctant victims. The offenders sought money, electronics, and a victim’s personally identifiable information (PII). This theme also includes offender moves designed to produce compliance with requests that were not overly emotionally laden or intricate (e.g., simply lowering the amount of the request). In all cases I investigated for this thesis, the offender swindled or attempted to swindle the victim. Table 7 offers additional quotes under this theme.

Table 7. Quotes Supporting Codes under the “Swindling” Theme

2nd Order Themes	1st Order Codes	Label	Quotes Supporting Code
Swindling	<i>Gathering Personal Information</i>	AS1	“Full name, Address, Bank name, Account number, Routing number, Bank login. Baby I want you to send me the details asap” (To AV1.1, May 2020).
		AS2	“Do you visit the account on the computer with the Amazon website?” “Then do you still know the login I’d and password to put in your account on the site?” “Okay what’s it ?” (To AV2.1, September 2018).
		AS3	“So how much are you looking at making ?” (To AV3, November 2016).
	<i>Requesting Money</i>	AS1	“Pls i want you to pick up the 300 on OneVanilla” (To AV1.1, August 2020).
		AS2	“Honey please will you be able to help me send at least \$100 To attorney ?” (To AV2.1, March 2019).
		AS3	“he just need help” (Transcript of Police Interview of AV3, August 2017).
	<i>Persuading</i>	AS1	“i need to send to mom for her surgery” (To AV1.1, August 2020).
		AS2	“And why is it now that I need \$\$ For [son] you have to do all this honey ?” (To AV2.1, March 2019).
		AS3	“Push push” (AV3 to AS3, November 2016).

a. Gathering Personal Information

In 20 of the 26 cases examined, the offender acquired or attempted to acquire sensitive personal data about the victim. This information could include the victim’s full name, date of birth, and other sensitive personally identifiable information. Offenders also sought to obtain login information for bank accounts, cell phone companies, and email accounts. Offenders also requested photos from victims. These photos could be used in future scams targeting other individuals.

One offender inquired, “Honey what is your full name ?” followed by, “What is your mother maiden name ?” (AS1 to AV1.21, May 2020). The offender sometimes peppered the victim with a variety of questions. In this example, an offender asked a victim, “When is your birthday?” “Where were you born and raised?” “Baby what is your home address honey” “What is your Employment status?” “Babe what is your total annual

income honey?” “Baby what is your mother maiden name ?” “baby what is your SSN ?” (AS1 to AV1.5, April 2020).

Occasionally, an offender tried to mask their request for information as when one offender wrote, “Well we all are humans and we have different emotions but most things we really need to talk about like the date of births and all mine is on the 27th of January and [son] is on the 24th of November how about yours ?” (AS2 to AV2.7, November 2019). Other times, the requests were straightforward, though not perhaps obvious to the victim. One offender asked a victim, “do you have a bank account ?” (AS1 to AV1.7, November 2019). Another offender asked, “What phone cellular do you use” (AS2 to AV2.16, June 2018).

b. Requesting Money

A romance scam is, at its core, an attempt to defraud a victim of items of value. Because the victim and offender are physically distant, the offender must induce the victim to provide the item of value willingly. The offenders accomplished this by making a request of the victim. That request was predicated on the premises that the offender previously laid out and the relationship the victim perceived with the persona. The offenders often requested a gift card, money, or a similar mechanism for value transfer from the victim. Though a variety of mechanisms to transfer value were seen in the data, the code was titled “Requesting Money” to emphasize the core idea that the offender intended to profit monetarily from the interaction. Requesting money was present in 22 of 26 cases.

Sometimes the requests were very straightforward. The offender asked for a gift card, “\$75 on Amazon” (AS1 to AS1.6, June 2020) or “Can you get \$50 steam ?” (AS2 to AS2.1, July 2019). Another request for money was simply, “I need \$376” (AS2 to AV2.3, January 2020).

Other times, the offender brought in elements of past stories. One offender texted, “Are you going to borrow me the \$7850 to pay book my flight a f start moving my things and pay my mom surgery when the big check comes you will get your money back” (AS1 to AV1.1, May 2020). Likewise, an offender asked, “Can you spare me 200 I wanna get

some items for my workers” (AS1 to AV1.9, April 2020). These types of requests appear intended to fit seamlessly with past premises the victim had already accepted.

An offender often used their intimate knowledge of the victim’s plans to situate a request for money. An example is an offender asking a victim, “Can you send me pick up 50 Amazon for me on your way back home honey” (AS1 to AV1.3, June 2020). Another time the offender wrote, “And pls I help me pick up an Amazon card on your way home I want to do another phone plans. \$75 on Amazon” (AS1 to AV1.6, June 2020). In this way the offender incorporated their exploitation into the victim’s daily activities.

Although the requests are often small, some victims lost significant amounts of money. One victim reported, “the first money went over to pay attorney’s, attorney’s retainer, and that was \$45,000 or close to that and I did it. That was a wire.” (Interview of PV2, September 2022). In another instance, a victim reported losing \$500,000 (Transcript of Police Interview of AV3, August 2017). Thus, victims can lose substantial amounts of money to romance scams.

c. Persuading

After requesting an item of value, an offender may use persuasive techniques to gain compliance from a victim. Monica Whitty created a model of romance scams that mapped out various persuasive techniques she observed offenders using in her research.¹⁴⁴ Whitty’s research impacted the development of the “persuading” code in this study. Persuading appeared in 23 of the cases.

“Persuading” as I observed it in this study occurred after a specific request for an item of value. Offenders used persuasion in an attempt to gain victim compliance with their requests. Persuasion includes forms of motivation from bargaining to begging to insistence, pushing, or waiting patiently. Persuasion is differentiated from “manipulating emotions” because the persuasion techniques are also observed outside of romance scams. Speech that is only motivating in the context of romantic relationships was coded as “manipulating moods.”

¹⁴⁴ Whitty, “The Scammers Persuasive Techniques Model.”

Offenders were sometimes straightforward in begging as when one offender texted, “Pls I’m begging you I will pay you back with interest” (AS1 to AV1.1, May 2020). Offenders were sometimes more imperative such as when one insisted, “You have to help honey” (AS2 to AV2.1, March 2019). As noted earlier, the offender sometimes incorporated previous assertions in their persuasive request like when an offender begged, “Babe pls I’m flat broke and I dont any food items for me and my puppies pls honey” (AS1 to AV1.6, June 2020). One victim reported that she felt the subject was “pushing really hard” (Interview of PV2, September 2022).

An offender sometimes used time pressure such as messaging, “I need it urgently” (AS2 to AV2.8, January 2020). They were also sometimes insistent. For instance, one offender demanded, “I want you to call Verizon customer service right now and ask then to set up Babe what is your Verizon username and password, Security questions and answers” (AS1 to AV1.3, May 2020). An offender commonly blended persuasion into an amalgamation of insistence such as, “You said 4 days and it’s 4th day today and you’re saying Wednesday again” “Do you have the \$100 now honey?” “Honey if you don’t send the money now I might probably not be allowed home anymore” (AS2 to AV2.3, September 2019).

Offenders might adjust the amount of their request, like an offender’s question “So which can you afford now honey ?” (AS2 to AV2.4, November 2019). Offenders also sometimes claimed they would pay the victim back. One victim reported the offender told him, “I’ll pay you back as soon as I get back you know when I get my money there. No, I’m not a liar. I’ll pay you back everything I owe you” (Interview of PV3, October 2022). Some victims appeared to find the concept that the money is a loan to be reassuring and safer than simply handing over the money without a promise to repay.

2. Money Laundering

Beyond swindling, offenders sometimes used or attempted to use victims as money mules. When this occurred, the offender first introduced relevant premises explaining the money flow. The offender next prepared the money mule to receive the funds by informing them how and when the money would arrive. Finally, after a money mule received the

funds, the offender directed the victim to transfer the money to another account using a method prescribed by the offender. Quotes illustrating this theme are provided in Table 8.

Table 8. Quotes Supporting Codes under the “Money Laundering” Theme

2nd Order Themes	1st Order Codes	Label	Quotes Supporting Code
Money Laundering	<i>Preparing for the Movement of Money</i>	AS1	“They will proceed with the payment today my love and the money is going to ge deposited to your account as soon as possible” (To AV1.1, August 2020).
		AS2	“Name: [IDNAME1] State: OH City: [City] Zipcode: [ZIP] Amount:\$250” “Did you get it babe” (To AV2.1, June 2019).
		AS3	“If the 11410 doesn’t show up today you might have to complain at the bank ?????” (To AV3, November 2016).
	<i>Directing the Movement of Money</i>	AS1	“Baby we are sending \$9000 to mom and you use \$1000 to pay off the bills get some items for [son] and you” (To AV1.1, August 2020).
		AS2	“Honey you’re not going to [Western Union] ...you’re just getting that card.” “You get one single of \$1000 and one single of 900” (To AV2.1, May 2019).
		AS3	“Western union\nName: AS3.5 \nAmount: \$3000\nState: Dubai\nCountry: United Arab Emirates\n\nMoneygram \nName: AS3.3 \nAmount: \$2000\nState: Dubai\nCountry: United Arab Emirates” (To AV3, November 2016).

a. Preparing for the Movement of Money

Preparing for the movement of money encompasses the offender providing general directions in advance of the money mule’s anticipated receipt of funds or items of value. The code includes providing directions to the money mule regarding the opening of financial accounts intended to be used for the future collection and distribution of fraud funds. The “preparing for the movement of money” code is differentiated from the “crafting and reasserting premises” code by the narrower purpose of the stories and premises the offender advances. These stories are intended to explain why the victim is receiving money from a third party. The codes also vary because the “preparing for the

movement of money” code contains objectively true facts. In the crafting and reasserting premises phase, all assertions are fictional tales meant to prime the victim for exploitation. Under this code, believing the victim is primed, the offender attempts to operationalize the individual and obtain the individual’s assistance in laundering money. Preparing for the movement of money was observed in 11 cases.

The offender provided explanations as to why the victim would be receiving funds from a third party. The offender often used previously established premises in crafting these explanations. For example, an offender asked a victim, “Can I trust you with my funds cause when I travel to get my fabrics I will like you to be helping to cash some money and pay as I get buy my fabrics and you can also book my flight with it” (AS1 to AV1.5, April 2020). The same offender told a different victim, “I want you help me cash my payment and you can book for my flight and hotel” (AS1 to AV1.3, May 2020). A different time this offender told a third victim, “i want you to help me cash some money from my lawyer” (AS1 to AV1.7 November 2020). A final example drawn from this offender was the offer that, “If you dont have money I can send you some money to book a flight for me” (AS1 to AV1.9, April 2020).

The offender normally gave notice to the victim when the victim should expect a deposit. An example is a suspect letting a victim know “You are going to be getting some payment today or tomorrow” (AS1 to AV1.1, August 2020). Occasionally, the offender told the victim they could keep a portion of the transfer. For example, one offender said, “I will be giving yoh 5% of every transactions” (AS1 to AV1.8, July 2020).

Money was not only transferred through the banking system. The offender sometimes directed the money mule to use the mail, such as with this offender texting, “Okay honey did you see that Information of \$150 I sent you to pick up at Walmart ? Pick it and then withdraw money from bank you should have \$439 to mail all packages” (AS2 to AV2.1 July 2019). Thus, money that was transferred through a money service bureau was converted to cash and forwarded outside the traditional financial system.

Offenders sometimes had money mules set up new bank accounts. For example, one suspect asked, “Is there any USAA bank closer so you can just open that or what do you think ?” (AS2 to AV2.1, May 2019). Another victim reported that the offender “asked

me to set up a separate bank account to be able to be used to send him money or receive money” (Interview of PV2, September 2022). These accounts served as additional locations to deposit funds as well as backup in case other accounts are closed.

Previously introduced characters were sometimes involved at this stage. For instance, one suspect confirmed with a victim that the suspect’s “lawyer” told her, “you will have to help me receive some \$\$ into your bank then withdraw and send to him once his traveling to the country to make the first initial deposit out of the requested amount needed to release the funds ..because his bank won’t accept funds transfer from one of the share holders that agreed to pay his debt first” (AS2 to AV2.4, November 2019). This use of repetition aided the victim in understanding the reasons for receiving money and accepting them as true.

However, not all of the offender’s preparation for money laundering paid off. Victims frequently rejected an offender’s requests, claims, and assertions at this stage, as demonstrated in Chapter IV. Victims’ rejection of requests demonstrates that even after grooming for exploitation, the victims were not mindless drones who acceded to every request.

b. Directing the Movement of Money

Directing the movement of money spans from the moment the money mule has received fraud funds until the funds are available to the next person. The offender provided explicit directions to the money mule regarding the collection and distribution of funds or items of value that were fraudulently obtained from a third party. The activities corresponded to a money laundering scheme’s placement and layering stages. Directing the movement of money also captures moments when a money mule or victim participates in a third-party fraud by converting a check or credit card number to cash or property. Although the conversion itself may not be traditionally understood as money laundering, the subsequent transfer of that value to the offender or another person would be.

At this stage, the offender provided the money mule explicit directions as to what to do with third-party funds. An example is a suspect telling a money mule, “Baby i want you to transfer \$5000 to mom on this account” (AS1 to AV1.1, August 2020). As noted

under the “Preparing for the Movement of Money” code, the offender sometimes directs the money mule to transfer the funds through the mail. For instance, one suspect directed a victim, “[NAME] [ADDRESS] NY Please send it with usps. Send me the tracking when you mail the cash to the address for my lawyer” (AS1 to AV1.1, September 2020). Thus, the offender used multiple means for placement and layering of fraud funds.

The recipient of the laundered funds was sometimes located in foreign country. One suspect told the money mule to send funds to Nigeria by directing, “You’re sending \$2,500 ... City is IKEJA.” (AS2 to AV2.1, May 2019). Another offender told the money mule to wire money to South Africa. The offender texted, “Baby wire \$32k to [NAME] ... [ACCOUNT NUMBER] ... Rivonia, Johannesburg, South Africa 2191” (AS3 to AV3, December 2016). This finding is consistent with previously cited FBI and FATF information regarding the international movement of funds.

The offender and money mule sometimes conducted several transfers at approximately the same time. Here a suspect told the money mule, “So as we wait for this \$11410 to hit your account back I want you to do a quick western union and money gram of 5\$k from the new referrals that came in” (AS3 to AV3, November 2016). This demonstrates the speed and frequency with which money mules can be used to transfer fraud funds.

3. Problem-solving

Problem-solving involves attempts to ameliorate inhibitors to exploitation like barriers or the victim’s/mule’s inability to transfer value as directed. Here the victim or money mule is properly motivated to assist the offender but has encountered an extrinsic hurdle that must be surmounted to comply with the persona’s request. Problem-solving involves the offender transferring new skills or knowledge to the victim or mule. It may also involve collaboration between the offender and money mule to develop a story needed to surmount a third-party obstacle. When this occurs, money mules are deemed to be witting participants as they are intentionally lying to a government entity or financial institution to comply with the offender’s request or direction. See Table 9 for examples.

Table 9. Quotes Supporting Codes under the “Problem-solving” Theme

2nd Order Themes	1st Order Codes	Label	Quotes Supporting Code
Problem-solving	<i>Coaching</i>	AS1	“Your bank cant open a account for you without a routing number. Every account number has a routing number” (To AV1.1, May 2020).
		AS2	“Let me teach you how to take screenshots ...click on the lock button on the right side of your phone :iphone: and the upper volume on the left side of the phone together to take s screenshot” (To AV2.1, May 2019).
		AS3	“Western union is another service like money gram” (To AV3, November 2016).
	<i>Collaborating</i>	AS1	“but i told you that i spoke with [Bank Employee 1]” (To AV1.1, September 2020).
		AS2	“And honey you have to call that store to correct the name it’s supposed to be AS2.9 and not [MISSPELLED]” (To AV2.1, April 2019).
		AS3	“Let’s put heads together on what to tell the police” (To AV3, December 2016).

a. Coaching

When the victim or money mule expressed a lack of knowledge or skill, the offender sometimes engaged in coaching. The offender helped the victim or money mule obtain new knowledge or skills through training, encouragement, and development. The new knowledge or skills were aimed at equipping the victim or money mule to better aid in the scheme and transfer money.

Sometimes the knowledge related to simple technical issues. One offender told a victim, “Tell your son to teach you how you can screenshot my love” (AS1 to AV1.1, August 2020). Another offender directed a victim to “Go to your phone message settings and search on how to enable Mns” (AS2 to AV2.1, September 2018). The same offender later instructed the victim, “Let me teach you how to take screenshots ...click on the lock button on the right side of your phone :iphone: and the upper volume on the left side of the phone together to take s screenshot” (AS2 to AV2.1, May 2019). Although it may seem elementary, the offenders had the money mules send screenshots to confirm monetary transfers. Therefore, this ability was important to the offenders.

In some cases, offenders trained the victims or money mules how to use Bitcoin. One victim stated, “I sent it all Bitcoin and he showed me how to do it because I’m not technical” (Interview of PV1, September 2022). Another victim reported, “He had to educate me and sent me all these instructions and his wallet” (Interview of PV2, September 2022). The offender’s willingness to expend time and effort to train victims and money mules to use cryptocurrency likely demonstrates that the use of Bitcoin is an important method for offenders to transfer value.

b. Collaborating

Collaborating appeared infrequently in the offender’s text messages. Although it was present in all three cases where the victim became a witting money mule, it was only found in two of the remaining 23 cases. Collaborating captures moments the offender worked or attempted to work cooperatively with a victim or money mule to overcome third-party obstacles to monetary transfer regardless of whether the money belonged to the victim or to a third party.

The following interaction between an offender and money mule while the money mule was attempting to establish an account to transfer cryptocurrency illustrates how they collaborated:

Offender: I told you what to tell them babe
Money Mule: What is the primary use of bitcoin ? Is first question
Money Mule: What is my current source of income?
Offender: For savings and transactions
Offender: House building
Money Mule: Nature of outgoing usage ?
Offender: What are the options there ?
Money Mule: There are no options it’s just empty space
Money Mule: What is source of income
Offender: Building house construction
Money Mule: What about out going? Atm usage
Offender: For savings of bitcoin
Offender: And payment of building materials
Money Mule: Should I say anything else to make it sound better?
Offender: Yes
Money Mule: Coinsource: We have updated the status of your account to:
AWAITING REVIEW (Messages between AS2 and AV2.1, January 2020).

The money mule here was more than just a passive recipient of directions from the offender. Instead, the money mule was actively working through an account registration for the purposes of aiding the offender in transferring funds from a third party. Note also that the victim specifically asked the offender, “What is my current source of income?” rather than providing the victim’s actual source of income. This is an example of how the type of information that money mules obtain can be aggregated into a picture of their level of understanding of the scheme (i.e., witting vs. unwitting participation).

C. SUMMARY

Offenders initiate romance scams by presenting personas with attractive profile photos and fascinating stories about their supposed life and situation to intended victims. When an individual expresses interest in the persona, the offender expresses intimacy, passion, and commitment to build a romantic connection between the victim and the persona. This relationship is the basis for the rest of the scam.

As the relationship develops, the offender presents premises essential to the scheme’s progress. The premises could include promises to meet, accidents, or arrests in foreign locations. The offender repeats these premises numerous times in various ways. Along with premises, offenders introduce other characters that give the tales depth and additional opportunities for repetition of premises. Co-conspirators, who may interact with the victim by phone or email, sometimes play the other characters.

Eventually, the offender requests money. If successful, the offender will ask again later for more money. If the victim expresses that they do not have enough money to comply, the offender resorts to begging, pushing, bargaining, or other techniques to induce the victim to send money. If the victim claims to lack the knowledge or skill to transfer the money, the offender may adjust their requested transfer mode or coach the victim. Coaching may involve providing directions or videos meant to increase the victim’s ability in the necessary dimension.

The offender also introduces the concept of receiving money on their behalf. This request is couched in previous premises that are repeated. If the victim is willing, the offender details when to expect the incoming money. Once the victim, who is now a money

mule, receives the money, the offender provides directions on where and how to transfer the money. When the money mule confronts the offender about information received from police or bankers regarding an illegal source of the money, the offender makes flimsy excuses and relies on the relationship for compliance. As more money is sent, the offender and money mule actively collaborate to overcome obstacles, including banks and police.

Via this process, offenders guide some individuals through romance scams and into co-offending as money mules. The oft-repeated premises and romantic connection between the victim and the persona are the basis and justification the offender relies on when making exploitative requests that would be irrational in other contexts. In the next chapter, I detail the victims' responses to these premises and exploitative requests to understand how this manipulation affects the victims' decision-making and judgment.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. VICTIM AND MONEY MULE COMMUNICATIONS

This chapter examines how the victims responded to the offenders. As with Chapter III, I provide examples of language that backs up code formation in narrative and tabular formats. Again, this level of detail demonstrates how the data supports the codes.

The study found that victims experienced various outcomes, including unsuccessful grooming attempts, successful grooming as a romance scam victim, subsequent successful grooming as a money mule, and subsequent unsuccessful grooming as a money mule. I found that only three of the 25 victims included in the study acted as co-offenders. Significantly, I also found that co-offenders can perceive that they are facilitating a crime yet be blind to the reality that the entire relationship is a sham. In other words, the findings suggest that individuals involved in romance scams can be both victims and offenders simultaneously.

A. ENGAGING THE PERSONA

Engaging the persona encompasses a victim's unwitting contact and subsequent romantic relationship formation with an online fake persona. The data in this study suggests many victims experienced the loss of a significant other or were facing a severe illness, which led them to be open to a romantic relationship. Once the victim met the persona, they engaged in otherwise normal behavior such as sharing background information, likes, dislikes, hopes, and dreams.

As the relationship progressed, the offender presented the victims with numerous premises. The data indicates that victims did not blindly accept all the assertions the offender made via the persona. Instead, the victims evaluated the persona's credibility through questioning, online research, or other means. Often, victims received information from outside the scheme. Although it is not always possible from this study to know how many victims exited the scam before financial victimization, victims often confronted the offender with insights gained from others. All too often, victims accepted rather flimsy excuses from the offender. This finding may support the conclusion that once beliefs are formed, they are resistant to change.

1. Emotional Loneliness

Emotional loneliness was present in 15 of the 25 victims in this study. In eight of the archival cases and all three in-person cases, the victim experienced a loss to death or divorce. The victims I interviewed clearly attributed their vulnerability to the scam to their loss.

The data suggests that one needs to be careful with the idea that romance scam victims are simply lonely. Data in a few cases suggested some of the victims had robust social lives or family support. One victim in an archival case shared stories involving approximately 90 different people from family to friends and coworkers during the approximately 17-month relationship she had with the persona (AV2.1 text messages). Another victim I interviewed for this study reported having a close group of friends she spent time with (Interview of PV1, September 2022). Similarly, another interviewee had family support (Interview of PV2, September 2022). What was potentially missing from the victims' lives was a romantic partner. Buecker et al. report in their meta-analysis of loneliness that this is described as "emotional loneliness," which is discussed further in Chapter V.¹⁴⁵

Not all participants or archival cases in this study were actively seeking a romantic relationship on a dating website. One victim, for example, was approached by a scammer through a website for widows and widowers (Interview of PV1, September 2022). Another victim was apparently approached on Instagram. The victim texted, "you sent your number to me on Instagram" in response to the persona asking what his name was (AV1.5 to AS1, April 2020). This observation may argue for a theory that extends beyond relationship seeking to explain victimization in romance scams. Table 10 provides additional quotes related to this theme.

¹⁴⁵ Buecker et al., "Loneliness and the Big Five Personality Traits," 8–9.

Table 10. Quotes Supporting Codes under the
“Emotional Loneliness” Theme

2nd Order Themes	1st Order Codes	Label	Quotes Supporting Code
Emotional Loneliness	<i>Death</i>	AV1.1	Not Present
		AV2.1	Not Present
		AV3	Not Present
	<i>Divorce</i>	AV1.1	Not Present
		AV2.1	AS 2, “And did you check your ex husband jewelries ?” AV2.1, “Yes exs jewelry” (AV2.1 and AS2, September 2018).
		AV3	Not Present
	<i>Illness</i>	AV1.1	Not Present
		AV2.1	“I am internally great full to you that night when I got that bad news from the Doctor I really was going to take all those pills they gave ... your kind words saved my life that night” (To AS2, September 2018).
		AV3	Not Present
	<i>Non-specific Origin</i>	AV1.1	“You didn’t come back to me last night honey. It was a very lonely night” (To AS1, May 2020).
		AV2.1	“just very lonely” (To AS2, October 2018).
		AV3	Not Present

a. Death

The death of a romantic partner or close family member was observed in seven of the cases. As an example, one victim texted, “I haven’t been with a man since my husband’s been gone” (AV2.10 to AS2, January 2019). Another victim reported, “My husband started declining and died” (Interview of PV1, September 2022). A third victim stated, “Well, when my husband passed away, he had a long journey with cancer, when he passed in [YEAR] I was so lonely and you know, I was in a fog” (Interview of PV2, September 2022). The data suggest that the loss of an intimate relationship to death may be a factor in romance scam susceptibility.

b. Divorce

At least five victims were divorced at the time of the scam. One victim wrote, “I’m lonely to sweets and would love to meet you and wish that we could be ‘an item.’ My ex-wife almost destroyed me so I’m careful” (AV1.4 to AS1, September 2020). A victim I interviewed reported he felt he was vulnerable because, “I went from living in a house with

my wife and two kids to a one-bedroom apartment living on my own” (Interview of PV3, October 2022). Like death then, divorce appeared to make some victims vulnerable to romance scams.

c. Illness

Five victims also spoke of significant illnesses affecting them or a close family member. One victim texted, “I have to be honest there is a lot of men that can’t handle my inillness and my sister. [NAME] doing ok I heard her talking loud too someone that wasn’t even in my home” (AV2.19 to AS2, June 2018). Another victim explained to the persona, “And you know i don”“t have it right now believe me i would if i could why do you think im with my mom my cancer messed me up i have nothing pls dont leave” (AV2.2 to AS2, June 2019). Still another victim messaged, “But your never there i came to you cause i was scared about my surgery and the biopsies they had to send in out of all the guy friends i have i run to you for Comfort you are the only one that takes my fear away that i feel i got alot of support but not from the one i want i should have never contacted you im sorry” (AV2.3 to AS2, September 2019). Illness may increase romance scam susceptibility by highlighting the absence of close support in a victim’s life.

d. Non-specific Origin

Non-specific origin captures expression of loneliness with no clear antecedent or cause. The loneliness appears to be related to the victim’s desire to interact with the persona. However, as this portion of the study relied on historical data, I was unable to gather information on the specific factors that contributed to the individual’s experience of loneliness.

As an example, one victim expressed his loneliness by texting, “My night was good but lonely. I dreamt we were finally together. I miss you too” (AV1.1 to AS1, April 2020). Another victim wrote he was the “Same as before tired lonely” (AV1.2 to AS1, July 2020). A different victim declared, “I would like having a relationship if want one. I’m very lonely right now” (AV2.8 to AS2, December 2019). While the particular cause of the loneliness was not apparent in these instances, it is clear from their messages that these victims desired a relationship.

2. Developing and Maintaining a Relationship

Like the offender's language, developing and maintaining a relationship encompasses the creation of a romantic relationship between a persona and a victim. This theme includes expressions of positive and negative emotions associated with the formation and continuation of long-term, intimate relationships. Offenders later relied on the relationships when they made exploitive requests of the victim. Additional quotes supporting the development of codes in this theme are found in Table 11.

Table 11. Quotes Supporting Codes under the "Developing and Maintaining a Relationship" Theme

2nd Order Themes	1st Order Codes	Label	Quotes Supporting Code
Developing and Maintaining a Relationship	<i>Commitment</i>	AV1.1	"I cant wait to be with you and spend the rest of my life with you" (To AS1, August 2020).
		AV2.1	"I have no desire at all none what so ever to be with anyone else but you" (To AS2, November 2018).
		AV3	"I believe in God will make us together forever ????" (To AS3, November 2016).
	<i>Passion</i>	AV1.1	"We can make love and romance anytime you want" (To AS1, April 2020).
		AV2.1	"I breath harder and I bud want you to slowly kiss my neck and start to take my blouse off" (To AS2, November 2018).
		AV3	"But you still need I spoil you with hot sex?????" (To AS3, November 2016).
	<i>Intimacy</i>	AV1.1	"I wish you were too so I could feel you jump every time the thunder hit while I'm holding you in my arms" (To AS1, August 2020).
		AV2.1	"Remember did I tell you how crazy work was this past weekend" (To AS2, May 2019)
		AV3	"When you get so weak, I ll always close to you, give you best food, tell you how much God loves us, I am the angel god send to care and love you?????" (To AS3, November 2016).
	<i>Dissatisfaction</i>	AV1.1	"If I'm all you have then things need to change. I'm done with the games" (To AS1, August 2020).
		AV2.1	"You still don't talk like that to me" "Am very upset about it" (To AS2, July 2019).
		AV3	"I ll leave you and won't want to involve your things anymore" (To AS3, November 2016).

a. Commitment

Just like with the offenders, I used Alam's definition of commitment for coding this dimension of the scam. As previously noted, Alam said, "commitment in a relationship refers to whether there is understanding about the future and whether the partners see each other together in the long run."¹⁴⁶ Victims used language consistent with this definition in 17 of the 26 cases.

Victims commonly used marriage terms to describe the persona. One victim, for instance, texted, "I can't wait for my wife to come home. I'm so excited" (AV1.1 to AS1, August 2020). Another victim messaged, "I put you on my Facebook that I was engaged to you" (AV1.2 to AS1 July 2020). A money mule wrote, "You won't be never regret to have me as your lover, wife and partner, I believe I am the perfect lady for you??" (AV3 to AS3, November 2016). Referring to the persona as a spouse was one way victims demonstrated commitment to offenders.

Like language from the offenders, victims spoke of a perpetual relationship. One victim asked, "Babe would you want to spend the rest of your life with me ?" (AV1.3 to AS1, May 2020). Another victim wrote, "Want b with you forever" (AV1.9 to AS1, April 2020). Still another said, "Honey I want you and only you for the rest of my life." (AV2.4 to AS2, November 2019). Similar to referring to the persona as a spouse, the victim's use of long-term concepts to describe the relationship demonstrated commitment to the persona.

b. Passion

As with the coding of offender language, I applied the definition of "passion" that Alam reported in his research to language used by victims or money mules. According to Alam's research, "passion in a relationship is an intense feeling of love, affection, and desire."¹⁴⁷ Passion in this study included expressions of attraction based on a recipient's

¹⁴⁶ Alam, "Three Essays on Socially Engineered Attacks," 193.

¹⁴⁷ Alam, 193.

observations of photos that were texted or the statements of interview participants. For the sake of decorum, explicit descriptions of sex acts were not specifically cited as examples of passion, though they were present in many of the cases. Examples of language associated with passion were found in 21 of the cases.

One victim described the passion as “the pulling of heartstrings” (Interview of PV2, September 2022). Another victim wrote, “I can tell you that i feel a strong love for you” (AV2.2 to AS2, June 2019). The same victim later wrote, “Come here and text me i want to hear those sweet words from you that makes me feel that crazy love i feel for you and makes me all funny inside” (AV2.2 to AS2, July 2019). Another victim said, “We can make love and romance anytime you want” (AV1.1 to AS1, April 2020). Whether engaging in sexting or expressing longing, passion was present in the majority of cases.

c. Intimacy

The definition of the code for intimacy was also adopted from Alam’s research. Alam defined intimacy as “a feeling of being close, emotionally connected, and supported. It also means regular and meaningful communications.”¹⁴⁸ Intimacy also included apologies and efforts to restore closeness following arguments and disagreements between the persona and victim. I found examples of intimacy in all cases in this study.

Intimacy was sometimes demonstrated in simple expressions of love such as, “Love you so much honey” (AV1.1 to AS1, September 2020). In other instances, the frequency of communication demonstrated how the victim shared the details of their daily lives. Take the following exchange as an example:

Offender: I miss you so much
Offender: What time did you wake up
Victim: 6 o’clock had to let the dog out turn the lights off the house
Take our meeting read come in and just sat down for a cuppa coffee I love
you honey more than you’ll ever now

¹⁴⁸ Alam, 193.

Victim: I'm going to have to make breakfast here real quick and get ready for the day I still don't know what I'm going to do about your hair appointment I wish you would cancel that and do it on Saturday or some day next week in the afternoon so I could be with you I want your company passion and love

Offender: I wish im there stitting beside you having coffee with you

Victim: Me too babe me too it was so muggy out I had to turn the air on when I got up the dogs in the kitchen laying on the floor because it's probably the coolest place on the floor (AV1.2 to AS1, July 2020).

These types of intimate interactions were common in the messages. Another example is:

Offender: Are you there

Victim: Had to bring my son to the foot doctor he fell and hurt his ankle

Offender: Omg how is he doing now

Victim: Ok

Offender: How did he fell and hurt is ankle where did that happen and when did he feel and hurt is ankle

Victim: Playing with his sister and fell from the bed

Offender: Sorry honey

Offender: How is he feeling now honey I hope he is better my love

Victim: He is feeling fine just wanted to make sure nothing hidden wrong with his foot

Offender: I hope the doctor has attended to him

Victim: X-rays already waiting on the doctor

Offender: Okay babe

Offender: I'm so proud of you are a good man and a good father I cant wait to meet you and your kids (AV1.5 to AS1, April 2020).

As these examples indicate, the victims and offenders exchanged frequent intimate messages. These messages likely contributed to the victim's attachment to the persona.

d. Dissatisfaction

As with the offenders, I used the "dissatisfaction" code to capture the expression of negative emotions such as disappointment, gaslighting, and not fulfilling obligations within the context of an intimate relationship. Such conversations occurred quite often in the archival text messages and were also referenced during the in-person interviews.

Dissatisfaction appeared more often in the victim category than in the offender category. It was present in 19 of the 26 cases.

The messages sometimes expressed exasperation with the demands of the offender as when one victim wrote, “I’m tired of this short notice crap” (AV1.1 to AS1, July 2020). Another victim wrote, “I thought you was a nice lady you don’t sound too nice now I think you got to forget this” (AV1.21 to AS1, May 2020). Dissatisfaction sometimes caused victims to cease communications permanently or temporarily with the victim. One victim texted, “I deleted everything I blocked you from Hangouts you’re very pretty woman and I told you that I love you I just can’t afford you” (AV1.2 to AS1 July 2020). This demonstrates that victims could find a relationship unfulfilling without recognizing it is a scam.

Sometimes victims expressed unhappiness with the relationship that had nothing to do with the scam directly. One victim stated, “I cant do long distance relationships I need man to hold me” (AV2.15 to AS2, November 2019). Another victim wrote,

I’ve got something to say. I love you and always will!!!! It makes no difference if you’re talking to other men or even if you’re sleeping with someone. Because i’ve spent the last few days giving our relationship a lot of thought and i’ve decided that i’m just to old for you. Plain and simple!! Please don’t answer this, i now have to try and get over you like i’m trying to do with [DIFFERENT ROMANCE SCAM PERSONA]. I may as well say goodbye to 2 of the 3 people i love more than anything in the universe (AV1.6 to AS1 June 2020).

In these instances, it was the nature of the perceived relationship with the persona, not the fact it was a scam, that drove a wedge between victim and persona.

Sometimes victims were disappointed that a promise went unfulfilled as when one victim texted, “I was hoping we would be together this weekend” (AV1.9 to AS1 April 2020). Other victims felt they were being unfairly treated like when a victim stated, “You still don’t talk like that to me. Am very upset about it” (AV2.1 to AS2, July 2019). Another victim stated succinctly, “I just don’t trust you” (AV3 to AS3, December 2016). Thus,

victims placed “normal” expectations on the persona like keeping promises and being treated respectfully. A failure of the persona to fulfill these expectations led some to be dissatisfied.

In other instances, the victim left the relationship due to dissatisfaction, never knowing the relationship was a fraud. For example:

Well you think you know me so well... throwing a guilt trip at me. Your wrong on so many levels. I really shouldn't have to explain myself to you but since this is the last time we'll be texting here it is...Your right I haven't texted you but it's because you keep throwing these I love yous at me when I asked you numerous times to pull back. You dont know me you haven't even spoke to me on the phone never met in person so I find it a little bit to much. Since when I asked you to stop and you didn't listen I did the only thing I could. I chose to step back. We want different things you want a wife I'm not ready for that you want me to leave everything I have here to be with you and how can I do that when I barely know you. I truly hope you find what your looking for [AS2] I'm sorry it wasn't me. Please be safe and goodbye (AV2.7 to AS2 November 2019).

This demonstrates the victim had to be open to a long-term, long-distance relationship for the scam to successfully continue.

3. Assessing Credibility

“Assessing credibility” encompasses the victims’ or money mules’ ongoing assessments of the believability of the personas, the premises, and the validity of the personas’ requests. Victims accepted, questioned, or rejected premises. They also had to judge incoming information from outside the scheme against the offenders’ premises. Table 12 contains additional relevant quotes.

Table 12. Quotes Supporting Codes under the “Assessing Credibility” Theme

2nd Order Themes	1st Order Codes	Label	Quotes Supporting Code
Assessing Credibility	<i>Accepting Premises</i>	AV1.1	“Baby I’m so happy right now. I’m so sorry for ever having doubt. It just seemed to good to be true” (To AS1, August 2020).
		AV2.1	“I do believe you have a son [Name] and he should have his game that’s why I will send it to him I have to stay focused” (To AS2, September 2018).
		AV3	“So I am working really hard to make \$50k bribe” (To AS3, November 2016).
	<i>Questioning or Rejecting Premises</i>	AV1.1	“If I do have a routing number. I’m not sure I want to give it out” (To AS1, May 2020).
		AV2.1	“How can you love me when we have never met?” (To AS2, September 2018).
		AV3	“I don’t like you attitude, when things happened, your behavior isn’t like a normal person” (To AS3, December 2016).
	<i>Receiving Outside Information</i>	AV1.1	“Just wish you could understand my worry. My bank told me to wait. I have every right to feel the way I do” (To AS1, August 2020).
		AV2.1	“I called the bank and they want some one else to talk to me about what’s going on about account” (To AS2, May 2019).
		AV3	“Omg, police just came To my home, I was almost to be arrested, what are you doing?” (To AS3, December 2016).
	<i>Acknowledging Criminality</i>	AV1.1	“That money wasn’t real and it didn’t come from you. And it’s not even there anymore” “I’m really having doubts this is real anymore” (To AS1, August 2020).
		AV2.1	“And I do know all about the iTunes and amazon scam so you can stop trying” (To AS2, September 2018).
		AV3	“The money deposit in my account on September 28, the amount \$205,704.11 was stolen money, they asked me pay back” (To AS3, December 2016).

a. Accepting Premises

For a relationship to develop and eventual exploitation to occur, the victims had to accept many premises that the offender advanced. “Accepting premises” captures acceptance that is expressed explicitly or implicitly by the victim. Implicit acceptance was seen when the victim reacted congruently with emotionally manipulative stories told by the persona. This code was found in all cases I reviewed.

The victims sent messages appearing to indicate they had accepted certain claims the offenders made via the persona. For instance, one victim asked, “What do you have planned for today are you going to do some more work on your sales try to get more money coming in” (AV1.2 to AS1, July 2020). This same victim abandoned a different potentially scam relationship in favor of the offender. The victim wrote, “[DIFFERENT PERSONA] has been blocked I’ve been thinking about all the red flags that I just bypassed falling for somebody. I don’t know I was kind of hoping that we could start a relationship tell me you love me and then you disappear” (AV1.2 to AS1, July 2020). Victims also accepted that the personality the offender advanced for the persona was valid, such as when one victim texted, “You sound like a good person. I think we would be good for each other” (AV2.8 to AS2, December 2019). These messages indicate the victims found aspects of the persona’s personality and purported activities to be believable.

Victims generally accepted the purported location of the persona. This can be seen in conversations with personas that victims believe are in the military such as when one victim wrote, “Be careful over there I know it’s got to be f***** up over there” (AV2.10 to AS2, December 2018). Another victim asked, “where u gonna live when u can leave Afghanistan” (AV2.16 to AS2, June 2018). This acceptance may set the stage for later exploitative requests based on these premises.

Victims also often accepted the persona’s purported employment. As in this example,

Victim:	What time do you have to go out on patrol?
Offender:	That’s later in the midnight
Victim:	Please be careful.
Offender:	That’s for sure ! (AV2.7 to AS2, November 2019).

Because offenders wove the employment-related premises throughout the scheme, a victim's acceptance of this premise, too, set the stage for the offender to use it to their advantage.

The victims I interviewed were candid about having missed cues they were being deceived. One money mule stated, "once people you know, fall in love, is blind" (Transcript of Police Interview of AV3, August 2017). Another victim said, "And then I think, 'Well, what if it's just that tiny little grain of sand?' What if it's real and I'm you know hurting this person? And I'm a caring, loving kind person. That's probably why I got sucked right into it" (Interview of PV1, September 2022). A different victim stated, "I thought, 'No, this is real'" (Interview of PV2, September 2022). Still another victim said the persona "sounded very suspicious, but I put that in the back of my head and didn't listen to it" (Interview of PV3, October 2022). Thus, victims ignored red flags and accepted the offender's premises.

b. Questioning or Rejecting Premises

The data in this study suggested that the victims do not just blindly accept the stories and premises advanced by the persona. In fact, "questioning or rejecting premises" was found in all cases I reviewed. Frequently, the victims questioned or outright rejected some or all of the offenders' premises. However, this questioning or rejection did not necessarily lead to full recognition of the scam or abandonment of the relationship.

Certain sensitive information seemed to be a trigger for questioning. One money mule wrote in response to a request for banking information that, "If I do have a routing number. I'm not sure I want to give it out" (AV1.1 to AS1, May 2020). Another victim asked, "My social security number why do you want that? already gave you too much information why you want my social security number?" (AV1.21 to AS1, May 2020). These exchanges demonstrate that victims do not comply with all requests or accept all premises even as they are being groomed and forming a relationship with the persona.

The relationship itself was sometimes called into question. One victim inquired, "I am still trying to understand how a beautiful woman like you could like an old man like me" (AV1.8 to AS1, June 2020). A different victim noted, "Sometimes I think because

western union told me that was woman picking up money maybe that is your woman” (AV2.1 to AS2, April 2019). While the victim may point out these concerns, it is common for them to accept the explanations provided by the offender.

Sometimes the request for money triggered a response like when one victim asserted, “I am not sending money. I’m not stupid” (AV1.4 to AS1, November 2020). A different victim took the denial to send money further by texting,

I don’t have time for all this b***** either you want to be friends and talk are you looking for somebody to send you some money or a credit card or something and that ain’t me the struggle is real out here should I’m about to start doing s*** I shouldn’t even be thinking about doing not with my body either have to start slinging s*** around out here and I know how that game goes it’s real (AV2.10 to AS2, January 2019).

Importantly, neither of these victims ended the relationship at this point, despite noting the inappropriateness of the persona’s monetary request.

Some victims questioned the reality of the persona like this victim who demanded, “Show me your even real in order for me i need a ring proving me things are real with us and you cant do that or me see you. Ive never even have seen you or will” (AV2.2 to AS2, June 2019). One victim started researching the persona’s purported identity. In this instance, the offender had stolen the identity of a money mule and used it for the next persona. This resulted in the offender presenting a male persona to one person and a female persona to another. The victim, when investigating, found discrepancies and confronted the offender with, “So you live in Minnesota now I’m just trying to figure something out is only one [NAME] how old are you” (AV2.9 to AS2, December 2019). One victim reported trying to determine whether the persona was real by “asking her to send me a selfie with you know, like your tongue sticking out. Or, you know, send me a selfie with your right hand touching her nose” (Interview of PV3, October 2022). Often the offender could counter even these concerns about their identity.

Sometimes the victim was uncomfortable with the direction the background premise took and the information provided by the offender. One victim stated, “that’s not my business were now venturing into an area that honestly I’m not comfortable with. You have to understand my concerns and suspicions this is all bit crazy” (AV2.7 to AS2,

November 2019). This demonstrates the importance of the offender providing stories and tales that smoothly interconnected with both past premises and the victim's comfort and experience.

c. Receiving Outside Information

In 17 of the 26 cases, data suggested the victim received information from outside the scam. This “receiving outside information” code is differentiated from the “providing characters” code by the source of the data. Information tending to be from a scam source while appearing to be another person was coded to the “providing characters” code. The “receiving outside information” code was then reserved for moments when the victim received factual information. The source of the information was sometimes human and other times the internet. This code also captures attempts to confirm information posited by the offender. Receiving outside information also includes prior victimizations that the victim claims to have learned from. Disinformation advanced by an offender's co-conspirator in the guise of a character was coded under the offender's “inducing gullibility” theme.

The internet was a common source for outside information. One victim wrote, “Good luck may God bless you if you think you're going to get away with everything google your 160 some pounds and you're 5 foot five wow and you same birthday and same place of birth sure I don't make sense to me who are you really,” (AV1.2 to AS1 November 2020). A victim I interviewed used the internet on her own to confirm elements of the premise being advanced by the offender. She said she “looked up to see if this was a new dictatorship” (Interview of PV1, September 2022). Thus, victims used the internet to fact check. However, the internet sometimes reinforced elements of the offender's tale and made them appear more credible.

Experience as a scam victim was also a source of information. An example of prior victimization included a victim relaying to the persona information about previous online relationships. The victim wrote, “They mostly ended up being scam just wanted phone upgrades phone cards steam cards Amazon cards and me to send money for them to buy a plane ticket” (AV1.5 to AS1, April 2020). Thus, even when victims have experience with

scams outside the current relationship, this knowledge may not result in skepticism towards the current persona.

Ironically, one money mule was even taking classes in money laundering. She wrote, “Tommrow I have another class I’m taking. It is on money laundrying. How they do that at casinos and how do I spot the people and help security” (AV2.1 to AS2, November 2018). The offender replied, “Well you going to teach me what you learnt from money laundering :wink::wink:” (AS2 to AV2.1, November 2018). This money mule eventually became a witting accomplice. Therefore, this is an example of how outside information can result in the money mule having sufficient understanding of their activities to eventually understand aspects of the criminal nature of monetary transfers.

Bankers and police were a common source of outside information. One money mule wrote, “Ok I talk to bank they said lawyer is fraud and [VICTIM] wants his money back who ever that is from lawyer. Bank lady said said this is a scam” (AV2.1 to AS2, May 2019). The same money mule also received information about the scam from the police. She wrote, “The police came over,” (AV2.1 to AS2, January 2020). Another money mule wrote, “Stop arguing with me my love I’m not a dummy. I can’t get the money out I tried it’s not really there. I went right to my bank. It made me look like a fool. I’m not happy” (AV1.1 to AS1, August 2020). Often police and bankers provided outside information on money laundering that raised concerns for money mules.

A victim in one case received information from a different victim. She wrote, “I need to ask you and i need you to be honest and explain a girl on my notificatons on fb left me watch out he is a heart breaker why would she put that?” (AV2.2 to AS2, June 2019). A different victim learned from her cell phone provider. She wrote, “AT&T TOLD ME WEDNESDAY ALL ABOYT IT” (AV2.4 to AS2, December 2019).

The victim’s family was also a source of information for the victim. This victim confronted the persona with,

Ok apparently you think I’m an idiot..If your going to tell this incredible bull of a story maybe you should have really read my text. You dont think I wouldn’t check. My son was in the military I told you this your rank first of all doesn’t exist it stops a an e9 there is no e18. Second it is against the law for your CO to with hold food and ammo. Plus we’ve been in Kubal for

over 14 years so were pretty established there for you to get what you need they supply you with food. Most important no commander is going to jeopardize going to Ft. Levenworth over a bag a gold. So dont text me as a matter of fact lose my number. Did you really think I was that gullible that I would send money and that I wouldn't check your story, (AV2.7 to AS2 November 2019).

One victim I interviewed related how her family used the internet to try to convince her she was being scammed. She stated,

my son in law is an IT guy. So he reversed imaged him [the persona], and they did an intervention with me at my house. The two kids and their husbands came in my son was on the phone and they showed me that this guy had taken photos from a guy in Germany's Facebook page to share with me and so they thought I was gonna be really mad at them. I'm not mad at you. Thank you so much for your love (Interview of PV2, September 2022).

Though the outside information was often relevant and apparently revelatory, offenders were frequently able to overcome information from outside sources and convince victims and money mules to continue in the scheme.

d. Acknowledging Criminality

"Acknowledging criminality" captured moments when the victim or money mule became sensitive to cues that the offender is untrustworthy to the point that they can no longer ignore or dismiss the cues. At this point, the victim or mule became conscious or aware of some aspect of the fraud. This recognition was coded the same whether the person was a victim or acting as a money mule. The presence of acknowledging criminality in a case demonstrates that the person was becoming sensible to an aspect of the overall scheme. This code was present in 13 cases. Some victims exited the scam at this point, while others chose to continue.

One money mule, to whom the offender had sent a credit card, noted, "The card isn't in your name" (AV1.1 to AS1, April 2020). The same money mule also discovered that money deposited to his account was not from the persona but was an "unemployment benefit applied for in my name" (AV1.1 to AS1, August 2020). Another victim similarly told an offender, "I didn't use the card number you gave me. I don't want to be accused of using someone card. If it had your name on it that one thing. But this just looked fishy to

me” (AV2.4 to AS2, November 2019). These victims and money mules detected direct indicators of fraud and lies the offender had told.

Victims were sometimes directly confrontational about the scam. One victim wrote, “Thank you for scamming me you taught me a real good lesson not to fall in love with women like you” (AV1.2 to AS1, November 2020). Another victim observed, “you sound like a scam” (AV1.21 to AS1, May 2020). These victims did apparently exit the scheme shortly after these realizations.

One of the money mules was seemingly even willing to engage in potentially treasonous behavior after recognizing several cues that the offender could not be trusted. The money mule wrote,

Please tell me who you really are and where you really live. Because by the sound of your voice and the way you speak your not from this country and that is ok with me. Honestly I think your not American and you need money to support your own army that is what I honestly believe and if that’s true you can trust me because I personally believe us should not be there. So that is what I believe who you are and I’m fine with that just tell me (AV2.1 to AS2 September 2018).

Later that same month, the victim asked, “Are you Afghan military???” (AV2.1 to AS2, September 2018). This is an example of a person understanding premises did not add up to the point they believed they were committing a crime. However, the money mule did not understand enough particulars to correctly identify the actual scheme and did not become skeptical that the lies told by the offender extended to the relationship itself.

On occasion, a victim or money mule directly inquired about money laundering. One money mule asked, “Tell me the truth, are you doing money Laundry? In God’s name” (AV3 to AS3, December 2016). Though the offender denied it, this is an example of a money mule correctly identifying the criminal activity they are participating in even if they do not know the origin of the money they are transferring.

A victim that I interviewed reported chatting with the offender after he had dropped his persona. She reported the offender said, “I’ll video with you one time.’ And it was at that time that I saw his face for the one and only time and the background was clearly a

very poor area of a foreign country and he was a very, very young black man” (Interview of PV2, September 2022).

B. ASSISTING THE PERSONA

After the victim developed a relationship with the persona, the offender made exploitative requests of the victim. At this stage, some victims recognized the scheme and exited it altogether. Others believed a romantic partner was asking them for help and responded consistently with relational norms, assisting the persona. The victim sometimes sent money directly to the offender, but that generally only occurred after the victim questioned why the money was needed. A primary distinction between assisting the persona and “engaging the persona” is that “real-world” consequences and actions often occurred. The victim sent their money or provided sensitive information about themselves. Although a victim engaging with the persona might have suffered emotional damage, those who continued through the phases in this dimension sometimes experienced monetary loss and engaged in criminal activity. A small number even continued with the criminal activity after recognizing it.

The data demonstrates that this is not an easy phase for the victim or money mules. They sometimes needed to overcome obstacles, endure hardships, and lie to police and financial institutions to comply with the offender’s requests. They expressed fear, anxiety, and other negative emotions as they did so. Therefore, continuing long-term in this phase required commitment on the victim or money mule’s part.

1. Helping a Loved One

“Helping a loved one” encompasses how the victims responded to the personas’ requests. In this interaction, the asymmetric nature of the relationship was observed. Having developed a relationship with the victim, the offender attempted to make money or obtain valuable information from the victim. The victims who complied with these requests believed they were in a romantic relationship with the persona. The victims judged the personas’ requests through that lens and may have believed they were being asked to help a loved one. The data shows that victims do not always blindly accept the requests and commonly revert to the “questioning or rejecting premises” phase. At this point, some

victims exited the scheme, thus potentially only suffering emotional, but not economic, loss. Table 13 contains additional quotes related to this theme.

Table 13. Quotes Supporting Codes under the
“Helping a Loved One” Theme

2nd Order Themes	1st Order Codes	Label	Quotes Supporting Code
Helping a Loved One	<i>Providing Personal Information</i>	AV1.1	“[Bank] in [City]. My address is [Address]” (To AS1, May 2020).
		AV2.1	“That is temporary password on top bank lady said” (To AS2, May 2019).
		AV3	“If the 2nd year there are 2–3 properties for sale, my income is \$1.5M before taxes” (To AS3, November 2016).
	<i>Sending the Victim’s Own Money</i>	AV1.1	“I got your [OneVanilla] card” (To AS1, July 2020).
		AV2.1	“I have 100 to spend” “Do you want 100 iTunes” (To AS2, September 2018).
		AV3	“every month I sent him \$5,000” (Transcript of Police Interview of AV3, August 2017).
	<i>Expresses a Lack of Means</i>	AV1.1	“I can’t even take care of me and [child]” (To AS1, May 2020).
		AV2.1	“I don’t have enough money” (To AS2, July 2019).
		AV3	“It’s hard to support him every month \$5,000” (Transcript of Police Interview of AV3, August 2017).
	<i>Expresses a Lack of Ability</i>	AV1.1	“Baby I’ve let you down today. Every time I tried to transfer the money through my phone it kept saying try later. So I’m still trying. If it doesn’t go through tonight. I’ll go to the bank first thing in the morning and have them transfer directly” (To AS1, August 2020).
		AV2.1	“Ok that’s not what it seemed like on u tube” “On how it worked” “I’m confused” (To AS2, June 2019).
		AV3	“What does mean \$2k money gram?” (To AS3, November 2016).

a. Providing Personal Information

In 18 of the 26 cases examined, the victim provided sensitive personal data to the offender. This information could include the victim's full name, date of birth, and other personally identifiable information (PII). Victims also provided login information for bank accounts, cell phone companies, and email accounts. Victims frequently provided pictures to offenders. These photos could be used in future scams targeting other individuals. I cannot provide quotes for this section without compromising the identity of the victims or money mules. Instead, Table 14 is a frequency chart showing how often victims provided sensitive information.

Table 14. Types and Frequencies of Sensitive Personal Identifiable Information Provided by Victims to Offenders

PII	# of Cases
Full Name	3
Date of Birth	7
Social Security Number	2
Bank Name	3
Bank Account number	4
Password	5
Income	5
Mother's Maiden Name	2

Note: The total number does not equal 18 because some victims sent more than one type of PII.

b. Sending the Victim's Own Money

Sending the victim's own money covers instances where victims transferred their own money or item of value. In 12 of the cases, victims sent their own money. The victims most often transferred money after a request from an offender that the offender predicated on a previously introduced and repeated premise.

The victims sometimes transferred value in the form of gift cards in the cases studied. For instance, one money mule wrote, "I got your 500 card" (AV1.1 to AS1, August 2020). Another money mule texted, "They only had 15 dollars and that was only card

besides uber” (AV2.1 to AS2, September 2018). Therefore, gift card were a means to transfer low dollar amounts.

Though the requests for money were frequently under \$100, some victims did lose more. One victim wrote, “you cost me \$5500 plus in the last few days” (AV1.2 to AS1, November 2020). Another victim reported sending, “\$5,000 out a time” (Interview of PV1, September 2022). Similarly, a victim I interviewed reported losing “probably in the neighborhood of 150,000” (Interview of PV2, September 2022). This demonstrates the substantial losses that victims can incur.

In two cases in the study, the victim or money mule first offered to send money based on the premises the offender presented. One victim proposed, “I should start sending a money order for [persona’s son] every pay check you think?” (AV2.1 to AS2, November 2018). A victim I interviewed similarly reported, “So that’s the interesting point. They never asked me for money. I offered” (Interview of PV1, September 2022). These examples establish that a well-crafted premises and grooming can induce some victims to offer money of their own volition.

c. Expresses a Lack of Means

The “Expresses a Lack of Means” code captures moments when the victim apparently accepted the request for value as valid, but maintained he or she had a lack of a sufficient supply of the requested value item to comply. “Expresses a lack of means” is differentiated from “expresses a lack of ability” because here the victim claimed only to have insufficient money to complete the request. They did not claim to not understand or be unable to comply. Expresses a lack of means is also differentiated from the “questioning or rejecting premises” since the victim appeared to accept the premise and subsequent request as valid. The victim simply reported they had inadequate means to fulfill the request. It should be noted there was no way to surmise from the data whether the victims truly lacked the means to comply with the request or used it as an excuse to for non-compliance. This code was present in 16 of the 26 cases.

Speech to express a lack of means tended to be quite plain. One victim wrote, “There is no way possible I can get that kind of money” (AV1.1 to AS1, July 2020).

Another victim asserted, “I really dont have the money babe” (AV1.3 to AS1, May 2020). A different victim replied to the persona’s request with, “Honey I would if I could but you know I don’t have any money I get 771.00 a month to live on and that it” (AV2.4 to AS2, November 2019). Sometimes, the victims alleged a lack of liquid assets such as when a victim texted, “I got money but it’s tied up and it’ll take me two weeks to get it out of there” (AV2.9 to AS2, December 2019). The victim’s expression of insufficient means often did not assuage the offender nor end requests for money.

d. Expresses a Lack of Ability

“Expresses a lack of ability” covers moments when the victim or money mule claimed they cannot comply with a request because they do not have sufficient knowledge or ability. The code is differentiated from the “questioning or rejecting premises” code because the victims here did accept the premise, they just did not have the ability to comply with it. This code was observed in all three money mule cases, plus four others.

For example, in reply to a request for banking information that a money mule did not understand, one victim wrote, “I’m old school honey. I don’t know how any of this works” (AV1.1 to AS1, May 2020). Another victim, explaining he did not understand how to buy an Amazon gift card stated, “I DONT KNOW HOW 2 DO ANY OF THAT STUFF” (AV2.16 to AS2, June 2018). These responses demonstrate that the victims accepted the offender’s premise, they just lacked the knowledge or ability to comply.

The offenders sometimes directed the victims or money mules to transfer money via Bitcoin. Some victims and money mules did not know how to conduct these transfers. One victim said simply, “And so I never use Bitcoin” (Interview of PV2, September 2022). Another money mule had to learn how to use Bitcoin. She communicated with the offender,

Money Mule: Did that have bitcoin ?
Offender: You should search on google bitcoin Atm near me
Offender: And see the nearest locations
Money Mule: Ok all these are all around now I understand
Money Mule: Are you sure you are coming here
Offender: Just put on google bitcoin atm around me
Money Mule: You didn’t answer me
Money Mule: I really don’t understand
Money Mule: When I do search to buy bitcoin card atm Anoka comes up

Money Mule: To use the other atms you showed me you have to have card already right?

Offender: You just need cash to use shy bitcoin atm

Money Mule: Ok that's not what it seemed like on u tube

Money Mule: On how it worked

Money Mule: I'm confused

Offender: Did you watch the video on how to purchase a bitcoin from a bitcoin atm (AV2.1 to AS2, June 2019).

As the example above illustrates, a money mule's or victim's expressed inability to complete a transfer sometimes led to the problem-solving phase.

2. Acting as a Money Mule

"Acting as a money mule" captures the money mule's transfer of money from initial preparations through the final transfer at the offender's direction. The funds being transferred under these codes included items that needed to be converted to be valuable (e.g., cashing a forged check, using a fraudulently obtained credit card) and other actions that were not money laundering but originated from a third party. A subsequent transfer of the money obtained by converting the item is money laundering; hence, those activities were included in this theme.

As noted elsewhere, when persons transfer money from a fraud scheme, they participate in money laundering. However, this theme by itself does not cover the critical issue of whether a money mule understands they are committing a crime. For a participant to be considered witting, the participant must recognize they are aiding a scheme, suspect an illegal source for the money they transfer, or believe the money will be used for an illegal purpose. Therefore, to define someone as a witting money mule, the codes "collaborating" or "acknowledging criminality" had to appear first. Table 15 contains additional quotes for codes under this theme.

Table 15. Quotes Supporting Codes under the
“Acting as a Money Mule” Theme

2nd Order Themes	1st Order Codes	Label	Quotes Supporting Code
Acting as a Money Mule	<i>Coordinating the Transfer of Incoming Money</i>	AV1.1	“That it’s 45,100 going into the account” (To AS1, August 2020).
		AV2.1	“I’ll just do bitcoin atm I’ll wait few days for Walgreens I will keep sending [Western Union] every few days” (To AS2, June 2019).
		AV3	“I will wire transfer to [Bank] on Monday, then Tuesday is immediately available ?????” (To AS3, November 2016).
	<i>Transferring Incoming Money as Directed</i>	AV1.1	“I just transferred 5000 to my checking” (To AS1, August 2020).
		AV2.1	Digital Mint Receipt: Deposited Cash: \$1050 Bitcoin Amount: 0.13681513” (To AS2, November 2019).
		AV3	“The MoneyGram went through, ready to pick up” (To AS3, November 2016).

a. Coordinating the Transfer of Incoming Money

The “coordinating the transfer of incoming money” code captures communications regarding the money mule’s participation in the preparatory phase of a specific money laundering act. The code includes acknowledging directions and the coordinating movement of money as directed. It is differentiated from “problem-solving” and “collaborating” because the money mule is following directions as opposed to proposing new ideas or potential plans to overcome problems. This code was present in all three cases where individuals acted as witting money mules, as well as five others.

In preparation to receive a transfer incoming fraud proceeds, a potential money mule sent their bank details to the offender. The victim texted, “bank routing number is [NUMBER] the account number is [NUMBER]” (AV1.9 to AS1, April 2020). One money mule inquired, “Baby how I’m I suppose to get 10,000\$ to you when the money is available” (AV1.1 to AS1, August 2020). Another money mule acknowledged directions for a money transfer via Western Union by texting, “Ok I’ll stop at the [CITY] wu at dollar general and send the first 900” (AV2.1 to AS2, May 2019). The final money mule provided an update to the offender by noting, “There are another \$16000 comes in” (AV3 to AS3,

November 2016). As can be seen, the money mules here are prepared to transfer money at the offender's direction.

Not all victims accept the premises related to money mule behavior. For example:

Offender: baby what is the name of your bank honey
Offender: i want you to help me cash some money from my lawyer
Victim: Find some one else I am not into that
Offender: okay thank you (AV1.7 and AS1, November 2020).

Here, again, the data demonstrated that simply being groomed does not imply blind acceptance of all premises or exploitative requests.

b. Transferring Incoming Money as Directed

"Transferring incoming money as directed" encompasses a money mule transferring value received from a third party at the direction of the persona or a character introduced by the persona. When conducting such a transfer, individuals acted as a money mule, not a fraud victim. This activity constitutes participation in a money laundering scheme's placement or layering stages, as described in Chapter I. This code was only found in the three cases involving witting money mules. Though victims may have acted as money mules in any of the other five cases under the "coordinating the transfer of incoming money" code, the data was insufficient to code them as definitively transferring money at the offender's direction.

Money mules commonly provided proof they had transferred the money as described. For instance, one money mule forwarded, "Hi [OFFENDER], I just sent you 370 USD. Cash will be available for pick up at a Western Union agent location now/by May 17, 2019. To pick up cash you need to <http://locations.westernunion.com/search/NG>. Thanks, [MONEY MULE]" (AV2.1 to AS2.1, May 2019). Other times, the money mule simply acknowledged having sent the money as when one money mule texted, "I deposited 900 I'll bitcoin the rest tomorrow" (AV2.1 to AS2.1, November 2019). Similarly, another money mule notified an offender she sent a "bank wire transfer \$30,550" (AV3 to AS3, November 2016). These statements clearly demonstrate the individual is acting as a money mule by transferring money as directed.

3. Problem-Solving

“Problem-solving” from the victim’s perspective involves removing barriers to transferring money regardless of the money’s source. As noted under the offender category, the victim or money mule is sufficiently motivated to assist the offender but has encountered an extrinsic hurdle that must be surmounted to comply with the persona’s request. Problem-solving involves the victim or money mule obtaining new knowledge or skills. It may also involve collaboration between the offender and the money mule to develop a story needed to surmount a third-party obstacle. When this occurred, I deemed the money mules to be witting participants as they intentionally lied to a government entity or financial institution to comply with the offender’s request or direction. Supplementary quotes related to this theme are listed in Table 16.

Table 16. Quotes Supporting Codes under the “Problem-solving” Theme

2nd Order Themes	1st Order Codes	Label	Quotes Supporting Code
Problem-solving	<i>Increasing Knowledge and Capabilities</i>	AV1.1	“I understand my love” (To AS1, September 2020).
		AV2.1	“I impressed with myself that I just figured out how to send that to you” (To AS2, May 2019).
		AV3	“Money gram is maximum \$1800” (To AS3, November 2016).
	<i>Collaborating</i>	AV1.1	“You have to call a different lady now. [Employee 1] is not the one any more. [Employee 2] is she took over now. Baby this is serious honey” (To AS1, September 2020).
		AV2.1	“She wants to know why I’m sending money to Nigeria?” (To AS2, May 2019).
		AV3	“Don’t let your clients use [Bank 1], try to\nUse [Bank 2]” “Ok baby” (To AS3, November 2016).
	<i>Persevering</i>	AV1.1	“Ok my love. Well I guess I have to go find a quick job to do then” (To AS1, July 2020).
		AV2.1	“This is very frustrating” (To AS2, January 2020).
		AV3	“I am so hungry and tired” (To AS3, November 2016).

a. *Increasing Knowledge and Capabilities*

The “increasing knowledge and capabilities” code appeared infrequently in the cases, though it was present in all three cases where the individual acted as a money mule.

The code includes moments when the victim worked with the persona or with the persona's encouragement to overcome a lack of ability to transfer value in the requested manner. It encompasses the acquisition of knowledge needed to perform the requested task. This code is the companion to the "coaching" code on the offender's side.

A victim I interviewed talked about learning how to use Bitcoin to transfer money. She said, "Well, initially, I was afraid of it. I really didn't want to do it and I struggled and hemmed and hawed. But afterwards, it's like, oh, I'm learning about Bitcoin. And some something new and it's, you know, contemporary and, you know, everyone's talking about it. I knew what a wallet was. I knew how to use a QR code to scan" (Interview of PV2, September 2022). This demonstrates a victim's ability to learn new skills in order to help the persona.

One money mule learned how to transfer money by Western Union and Bitcoin. Regarding Western Union, the money mule wrote, "You know that took 4 hours for me to figure out how to do that. The cashier guy helped" (AV2.1 to AS2, April 2019). A couple of months later, she texted, "Oh that makes sense now," after the offender instructed her to watch a video about how to use a Bitcoin ATM (AV2.1 to AS2, June 2019). A couple of days later, the money mule sent the following receipt via text message, "Digital Mint Receipt: Deposited Cash: \$260 Bitcoin" (AV2.1 to AS2, June 2019). This shows money mules may continue to improve their knowledge and skills over time.

Sometimes the new knowledge was simply learning about another business that could be used to transfer money to the offender. For instance, a money mule learned about Money Gram transfer rules after an offender told her the company was like Western Union. The money mule texted, "Money gram is maximum \$1800" (AV3 to AS3, November 2016). Thus, the money mule acquired knowledge that was later applied to transferring money efficiently through various systems.

b. Collaborating

Like with offenders, "collaborating" infrequently appeared in the victims' communications. Although present in all three cases where the victim became a witting money mule, collaborating was only found in three of the remaining 23 cases.

“Collaborating” captured moments a victim or money mule worked or attempted to work cooperatively with an offender to overcome third-party obstacles to monetary transfer, regardless of whether the money belonged to the victim or a third party.

The victims who did not become money mules reported trying to solve problems related to transferring money. One victim stated that the offender wanted her to transfer more than her bank’s daily limit of \$5,000. The offender reportedly asked her to get the bank to allow her to send \$8,000. The victim stated, “Well, one of the guys at the bank, [NAME], one time let me take \$7,000 out. And then he said, ‘that’s a one-time thing.’ And I said, ‘that’s fine’” (Interview of PV1, September 2022). Another victim expressed the effect this conversation had on her by stating, “with the attorney, I felt like I was becoming more part of the fold, helping [the persona] solve this problem that he had” (Interview of PV2, September 2022). Thus, victims worked with the offender to solve problems sending money.

The money mules’ collaboration included issues transferring money and coordinating messaging to police officers who were investigating. For example, a money mule wrote, “Omg, police just came to my home, I was almost to be arrested, what are you doing?... How should I answer their questions?” (AV3 to AS1, December 2016). The money mule later texted, “We are solving problems, if one day you don’t hear from me, then I am inn trouble , may in jail” (AV3 to AS1, December 2016). The following day, the conversation continued between the money mule and the offender:

Money Mule: Can I just send them an email to state, [CO-CONSPIRATOR] business partner [and] [PERSONA] did referral business online, he doesn’t know this money is stolen, he is working on it to get all these people involved, I will send you all details when I receive from him?

Money Mule: Do you think I should send them a message this morning like this?

Money Mule: I would say you know [CO-CONSPIRATOR] for almost 5 years, you are in Dubai, and you need a business account to receive your money for people who you are working with online.

Offender: Ok you can say that

Offender: Then I ll provide details soon

Offender: Don’t email them now, just wait a little before you email so you might email them together (AV3 to AS3, December 2016).

Here the money mule was clearly working with the offender to craft a message to give to the investigating officers.

c. Persevering

“Persevering” captures the emotional difficulties experienced by the victims and money mules. “Persevering” also includes physical problems such as long drives, fulfilling time-consuming requests, and similar issues. This code is differentiated from “dissatisfaction” because the frustration or issue the victim or money mule relays to the offender appeared to be aimed more at a situation or a request than at the overall relationship. This code appeared in seven cases, including all three cases where the individual acted as a money mule.

The stresses caused the victims to express anxiety and depression. One example is this exchange between a victim and an offender:

Victim: Your making me feel like shit.
Offender: Pls promise me you will do something tomorrow morning
she have to leave for her appointment by 10am
Offender: Baby pls dont feel like that okay
Victim: And after everything I’ve done for you and your mom
already
Offender: Baby I’m broke. My bills are behind. Winter is coming and
I can’t afford to get ready for it. I’m getting worried nervous and starting to
get depressed (AV1.1 and AS1, August 2020).

Other times, the financial stress of supporting the persona caused the victim to worry about fulfilling other obligations, such as with this exchange:

Victim: I’m at Walmart in [CITY] now but I m not going t
Offender: You’re not what ?
Victim: I only get the 1 card until Friday next check
Victim: Because of truck and money I had to give [RELATIVE] for
tabs
Offender: Honey get one \$100 google play gift cards
Victim: And fix truck
Victim: This is really stressing me
Offender: And one \$50 google play gift
Offender: You still have \$49 in card for gas
Victim: I mean this is really stressing me
Victim: What if I break down
Victim: I’m here by myself

Offender: You will still have extra cash with you if you buy \$150 card (AV2.1 and AS2, January 2019).

The emotional or time stresses caused by complying with the offender's requests even affected some individuals' appetite or ability to eat. One victim texted, "Honey I didn't eat anything at all yesterday and Friday I ate 3 French fries and 4 bits of a fish sandwich. My nerves are really tore up" (AV2.4 to AS2, December 2019). Similarly, a money mule wrote, "You see how selfish you showed me, only your stuffs, I have been hanging out for 4 hours, I haven't have my lunch yet, you only push me again and again. I am so hungry and tired" (AV3 to AS3, November 2016). Victims and money mules sometimes exhibited a willingness to overcome personal difficulties in order to help the persona.

C. SUMMARY

A review of the language used by romance scam victims and money mules indicates that many were susceptible to being scammed due to lacking a romantic partner. After meeting a persona that they find physically attractive online, they form a relationship by exchanging reciprocal expressions of intimacy, passion, and commitment. As the offender repeatedly presents premises to them about the persona's location, financial status, and current condition, the individual makes assessments of the persona's credibility.

Eventually, the individual faces a request for money. Those with the means, ability, and who have accepted enough premises, comply with the request and send money. Those lacking means may express that fact and enter a conversation, including persuasion from the offender. Individuals who do not have the ability may begin to problem-solve with the persona and be presented with coaching that is intended to increase their knowledge and capabilities.

Over time, the individual may be presented with premises related to receiving and sending money. If the offender can sufficiently explain the need for this activity within the context of the scam, the individual may begin to act as a money mule. This money mule activity leads to receiving outside information from authoritative sources like police and bankers that the individual is participating in fraud. When the individual confronts the persona with this information, the persona provides weak denials or excuses. Eventually,

despite receiving outside information and acknowledging several criminal aspects of the scheme, some individuals continue to receive and send money on behalf of the persona.

Overall, the language used by victims indicates that those who eventually choose to co-offend as money mules rely on the relationship for justification. Though these individuals receive credible information about the criminality of their actions and express significant doubts to the persona, they continue to participate in receiving and forwarding money. This choice appears to demonstrate that the individual remains unaware that they are in a scam relationship. In Chapter V, I draw on the psychological and criminological literature to explain why some individuals react this way.

V. THE PATH THROUGH ROMANCE SCAMS TO CO-OFFENDING

To effectively answer the research questions regarding the transformation of romance scam victims into money mules, I analyzed more than 134,000 historical text messages between three offenders and 22 victims. Three of these victims also intentionally aided the offender with money laundering as money mules and accounted for 87% of the text messages. This robust data set gave me a unique look into romance scams and the techniques offenders use to gain and maintain victim compliance. This data was augmented with three in-person interviews of additional romance scam victims. Though no one I interviewed had acted as a money mule, their experiences helped me develop deeper insights into the grooming and exploitation processes.

I consulted prior research on romance scams to begin developing a theory to explain my observations. I then elaborated on other theories, including grooming and gullibility, to encompass money mule behavior. This elaboration required using the more generalizable concept of “exploiting” rather than specific terms drawn from mass market fraud, as offered by Whitty. My view is that Whitty’s “Scammers Persuasive Techniques Model” explains one particular type of exploitation (i.e., theft) through a relevant lens. However, referring to Figure 2, Whitty did not directly incorporate all forms of exploitation into her model, as demonstrated by “sexual abuse” being to the side and money laundering being left out altogether.

I offer the “Path through Romance Scams to Co-offending” model to bridge the theoretical gap between theft and other types of exploitation seen in romance scams (see Figure 4). This model uses theories related to decision-making errors commonly grouped under the term “gullibility” to explain the grooming process. The model also leans on theories of “persuasion” advanced by Whitty, of relationship formation in romance scams from Alam, and of “emotional loneliness” relayed by Buecker et al. to situate the model I develop from the data I analyzed in the literature. The “Path through Romance Scams to Co-offending” model accounts for inputs from multiple scammers (i.e., it allows for a conspiracy) as it is focused on language that is presented by an offender via an online persona.

The theoretical constructs used to explain romance scams in prior literature, like gullibility, grooming, persuasion, and relationship-seeking, were broadly seen in my data and incorporated into the “Path through Romance Scams to Co-offending” model. I found those constructs could be sufficiently elaborated to explain victim behavior through acting as an unwitting money mule.¹⁴⁹ However, these constructs did not fit individuals who were no longer entirely gullible.¹⁵⁰ Instead of exiting the scheme at this point, these individuals collaborated with the offender or were consoled by weak reassurances from the offender despite some authoritative outside information like police contact or warnings from banks. The individuals then continued to act as money mules. I therefore concluded that a force other than gullibility or persuading (as the term is used in mass marketing) was at play.

To explain why a romance scam victim would continue to aid a persona after acknowledging they are committing a crime, I combine research on belief formation and co-offending with my data to propose a new grounded theory and a definition of “grooming.” Some research into co-offending offers individual personality traits and relational motives that may explain an individual’s decision. Meanwhile, research on belief formation offers insight into how a person can come to hold conflicting beliefs. Thus, the “Path through Romance Scams to Co-offending” model, and the related grounded theory offer a potential description and explanation of how individuals evolve through romance scams into unwitting money mules and then on to co-offenders.

¹⁴⁹ Note: The route an unwitting money mule takes in the “Path through Romance Scams to Co-offending” model includes an offender crafting and retelling a premise regarding receiving and sending money that the victim accepts as true. The victim then chooses to help the persona (i.e., loved one) by acting as a money mule and transferring money. The key difference between witting and unwitting then is the “acknowledging criminality” code combined with the degree to which the victim accepts, questions, or rejects the claims the offender makes that are intended to assuage the victim’s fears about criminal activity.

¹⁵⁰ Note: The decision-making process that includes being sensitive to an aspect of the scheme (i.e., potentially no longer fully gullible and thus acting as a witting money mule) is represented in the “Path through Romance Scams to Co-offending” model by individuals who, having reached the money mule phase, assess the credibility of a premise or some outside information, recognizes criminality, and rejects the claims the offender makes that are intended to assuage the victim’s fears about criminal activity.

A. HOW DO INDIVIDUALS BECOME MONEY MULES AFTER BEING VICTIMIZED IN ONLINE ROMANCE SCAMS?

My analysis suggests individuals who fall victim to online romance scams experience loneliness associated with the lack of a romantic relationship in their life. I noted that simply defining the victims as lonely did not appear accurate, as some of the victims had strong family ties and social networks. The victim's loneliness may stem from the loss of a loved one to death or divorce. The loneliness may also be related to a significant illness the individual is experiencing. Other times, no clear precursor for the loneliness was seen in the data, though victims express it. The loneliness appears to make the individual susceptible to approach by a scammer.

While in a susceptible state, the victim meets an offender online who is disguised behind a persona. The offender provides basic information for the persona like a name and age. Sometimes the offender uses an identity that was stolen from a different romance scam victim. In those instances, the offender may weave facts from the identity theft victim's real life into the persona's fake one. The offender also provides a photo, which is reciprocated by the victim. The victims usually find the photo the offender uses for the persona attractive. These photos are almost by always stolen as the offender is hiding behind a persona and would not want to reveal their face.

The offender also gives the persona a personality and life. The persona shares likes, dislikes, hopes, and dreams. The victim reciprocates the information sharing. Frequently, the offender tailors the persona's purported preferences to mirror the victim's preferences.

In addition to "who" the persona is, the offender asserts a location and source of income for the persona. The location is geographically distant from the victim and is used later as an excuse for delayed meeting. The offender also supplies information about the persona's financial stability and employment. The military is sometimes the reported employer. In many instances, the persona also claims to have a substantial inheritance. Regardless of the purported location or employment, these claims provide the offender excuses for later crises, delays in communication, and delays in meeting.

Through these initial interactions a relationship forms. The persona and victim begin to exchange expressions of intimacy, commitment, and passion. The persona

expresses love relatively early and often in the relationship. Individuals who stay on the path to co-offending appear to respond favorably to these expressions. The offender likewise makes frequent assertions of commitment. Over time, the victim and persona refer to each other in married terms calling each other husband and wife. They build an imagined future together that includes a home, children, and integration with the victim's existing family.

Despite the name, romance scams are not all romance. Victims and offenders frequently express dissatisfaction with the relationship. They disagree, argue, and threaten to end the relationship. They express jealousy or annoyance with one another. For the victims, these are likely genuine frustrations with the relationship. Some victims exit the scheme at this point without ever expressing they believed they were being setup for a scam. For the offender, this is potentially another means to make the relationship feel real and potentially motivate the victim through threats of relationship loss.

While the relationship builds, the offender begins to advance a series of premises. These premises serve as the basis for future requests for money. They often include travel to new location. The offender may likewise build on a previous claim of an inheritance by telling stories about why they cannot access it. The persona's stories frequently include details the victim finds interesting. The offender repeats these claims often and weaves them through other tales.

The victims respond to these premises with language that indicates acceptance, rejection, or questioning. When a premise is accepted, the offender may move on to another topic or elaborate the current premise. If a victim questions the premise, the offender often elucidates the premise further. Outright rejection or firm questioning by a victim causes the offender to explain away inconsistencies that the victim notes. These new premises or explanations are sometimes a simple refutation of the victim's concerns.

The offenders also introduce characters into their stories. They may include family, friends, and colleagues. Lawyers and bankers are two frequently mentioned characters. In time, the victims may interact by phone or email with real persons claiming to be one of the previously introduced characters. Offenders also may provide websites where the victim can login and observe the persona's bank account balance. Sometimes gifts are sent

by the offender to the victim. These characters and gifts all reinforce the premises the offender advances.

Interspersed throughout the courtship process, the offender gathers personal information about the victim. The accumulation of the victim's information may occur organically and subtly, or the offender may demand it and rely on the relationship as a justifiable basis for the request. The information gathered may include the victim's full name, date of birth, social security number, bank account numbers, and other valuable details. Victims commonly question the persona's need for this information. The offender may hide behind apparent reciprocity by providing fake or stolen personal identity information for the persona. In this way the offender gathers valuable data about the victim that can potentially be monetized later through activities like credit card applications or applications for unemployment.

Shortly before the offender requests money from the victim they often attempt to manipulate the victim's mood. This manipulation can be in either a positive or negative direction. Positive manipulation includes impending promises to meet or to obtain the purported inheritance. Negative manipulation includes emergencies such as an accident, illness, or imprisonment in a foreign country. The victims frequently express emotions that are congruent with the offender's manipulations.

The offender then makes a request for money. The money is frequently requested in gift card form. Sometimes the victims comply with the request, having accepted the necessary premises previously advanced by the offender. However, victims may reject these requests by claiming a lack of money themselves. Another reason victims give for rejecting requests for money is that they do not know how to transfer money via the method the offender has requested. The offender may respond to the rejection by begging, pushing, bargaining, or otherwise attempting to persuade the victim. The offender may also frame the monetary request as a loan. Some victims appear to feel a loan is less risky than giving the money away. This cycle of requesting money followed by the victim's varied response occurs many times with some victims sending substantial amounts of their own money to the offender.

Over time, the offender introduces premises related to receiving and transferring money. The offender builds these premises on prior premises like their inheritance or an arrest in a foreign country. Relevant characters like a lawyer or banker may be referenced and identified as the person who needs money to help the persona. The source of the money is portrayed as a business opportunity of some sort whether payment by an associate or other income-generating activity. The offender also weaves their location into this premise by claiming they cannot receive payment directly wherever they are. Victims evaluate these statements and may accept, question, or reject them bringing the offender back into the response cycle.

When a victim accepts the premises for receiving money from other people, the offender then arranges for fraud funds to be transferred to the victim, who has now become a money mule. The nature of the communications at this point changes to a degree since the offender must, for the first time, tell some truths. These truths relate to the timing and manner of the incoming money transfer. Once the money mule confirms receipt of the money, the offender directs the money mule how and where they should transfer the money. Here, again, the offender must reveal some truth by giving actual accounts where the money can be received. Methods of transfer money mules used in this study include mailing, money service bureau, wire transfer, and cryptocurrency transfer.

The money mule may not know how to transfer the money by the means the offender has requested. Using cryptocurrency, buying gift cards, and using money service bureaus like MoneyGram and Western Union are some examples of payment methods with which money mules may be unfamiliar. Unless the offender changes the means, the offender coaches the money mule. The offender may provide directions or videos explaining the process. Once the money mule obtains the new skill or knowledge, they can then transfer the money as requested.

Complying with the offender's requests takes a toll on the money mule. They experience anxiety, hunger, and exhaustion. They often need to find other sources of money since they may be simultaneously moving money for the offender while still providing some of their own. Despite these difficulties, the money mules carry on.

At any point in the scam, the victim or money mule may receive outside information. Common sources of outside information include family, financial institutions, banks, and government employees. The individual must then weigh the information the outside source has provided against what the offender is claiming. Frequently, the individual confronts the persona with the new information. The offender then cycles through repeating a prior premise, creating a new one, or providing some other explanation. Some romance scam victims exit the path at this point and thus avoid becoming money mules.

Money mules in long-term relationships receive outside information many times. This information sometimes comes from authoritative sources like financial institutions and police. Eventually, some money mules express their understanding that a crime is occurring to the offender. They may ask the offender about laundering money or reference previous instances where they learned the offender lied to them about the source of money. The offenders generally make weak denials and resort to expressions of love and commitment. The money mules tend to respond favorably to the offender and continue to assist while expressing apprehension. Importantly, while understanding they are being lied to by the offender about the money, the money mules do not recognize their entire relationship is with a fake persona.

After the money mule acknowledges the criminal nature of the transfers but chooses to continue, they may encounter problems with transferring money. Sometimes they collaborate with the offender by suggesting different routes or timing for the transfers. Other times, the money mule creates fictitious stories with the offender to tell law enforcement or a financial institution in an effort to conceal their activities. Having arrived at this point, a person has evolved from a romance scam victim to a witting money mule who acts as a co-offender in a money laundering scheme.

B. WHY DO ALL ONLINE ROMANCE SCAM VICTIMS NOT ACT AS MONEY MULES?

Individuals in this study who became money mules bypassed all the exits available to them on the path to co-offending. They overcame dissatisfaction with the relationship and accepted the offender's criminality. They engaged in long-term, committed

relationships with a persona animated by a scammer. Meanwhile, the substantial majority of individuals in the study left the relationship before becoming money mules. The victim leaving the scam does not indicate full understanding of the scheme on their part. It may be a recognition of an unreasonable or potentially abusive request. Thus, it is not just recognition of the persona as untrustworthy that is important but also what one does with it that matters. This may suggest a variance in personality type.

A comparison of the constituent cases that form the aggregate cases designated A1 and A2 in this study similarly suggests that the varied victim outcomes may be due to some victim circumstance. As a reminder, the offender in case A1 interacted with 75 different individuals while the case A2 offender interacted with 146. Out of all those interactions, only one co-offending money mule was identified in each case. Though the cases in this study were selected for theoretical contribution, not statistical purposes, one would expect more co-offending money mules would have been found if co-offending was linked to the offender's skill in recruiting. Therefore, I propose the difference in outcomes is due to some victim characteristic or condition.

C. DISCUSSION AND FUTURE RESEARCH QUESTIONS

The large data set I reviewed for this study gave me an expansive view into the techniques offenders use to exploit individuals in romance scams through theft and inducement to commit crimes. While my findings related to the initial romance scam portion of the victim's experience largely tracked with previous studies, my data set did provide some unique insights. For one, the data set allowed me to observe how the victims initially interacted with the persona and theorize how the victim's innate and situational susceptibility to romance scams interacts with the offender's portrayal of the persona's characteristics. I also observed the prominent role of repetition and defense of claims by the offender. These two findings allowed me to develop a nuanced view of grooming in this context and to propose a definition for grooming that incorporates theories of belief formation.

Finally, my data set allowed a deep dive into co-offending by a money mule who was first a romance scam victim. I have been unable to find previous research that delves as far into this aspect. Here my findings support the proposal of a grounded theory

regarding the phenomenon of a prior romance scam victim co-offending as a money mule with a persona they believe to be a romantic partner. Together, I believe these findings provide new and important theoretical insights into romance scams, money mules, and co-offending.

1. Victim Susceptibility

I find that Routine Activity Theory (RAT) is helpful in characterizing the initial offender-victim interactions in romance scams. Briefly, RAT is a concept from criminology that was advanced in 1979 by Cohen and Felson and has been since applied to the online environment through studies like the one by Pratt, Holtfreter, and Reisig.¹⁵¹ The theory states that crime victimization occurs when a “motivated offender” meets a “suitable target” in the absence of a “capable guardian.”¹⁵² The study found that RAT was useful for understanding how offenders target victims online specifically for fraud.¹⁵³ In the context of romance scams, the creation and animation of an online persona demonstrates the offender’s motivation. The victim’s engagement with the persona without recognizing the offender is behind it qualifies as suitability. Finally, the lack of a capable guardian is the absence of safeguards on the electronic platform through which the offender and victim communicate. I focus here only on the dimension of victim suitability to romance scams, as demonstrated by my data.

As noted previously, some individuals in this study expressed feeling lonely despite having a network of family and friends. Prior literature researching loneliness reveals similar observations. Buecker et al., citing research by Robert Weiss, explain that “emotional loneliness” includes a perceived deficit of intimate relationships such as romantic partners.¹⁵⁴ By comparison, “social loneliness” refers to the lack of a larger social network.¹⁵⁵ This differentiation is important when considering potential solutions or

¹⁵¹ Travis C. Pratt, Kristy Holtfreter, and Michael D. Reisig, “Routine Online Activity and Internet Fraud Targeting: Extending the Generality of Routine Activity Theory,” *Journal of Research in Crime and Delinquency* 47, no. 3 (August 2010): 269, <https://doi.org/10.1177/0022427810365903>.

¹⁵² Pratt, Holtfreter, and Reisig, 269.

¹⁵³ Pratt, Holtfreter, and Reisig, 281–85.

¹⁵⁴ Buecker et al., “Loneliness and the Big Five Personality Traits,” 8.

¹⁵⁵ Buecker et al., 9.

mitigating efforts for the problems of romance scams. Campaigns aimed at ending loneliness, while undoubtedly helpful for easing social loneliness, may not fully address romance scams because an individual may still specifically desire a romantic partner.

Serial romance scam victimization may also be in part due to emotional loneliness. Once victims exit romance scams, they lose romantic partners. Thus, victims may return to the same or a similar pre-scam condition that led to the previous fraud. Sorell and Whitty's findings support this idea. Following a romance scam, "sometimes the ruin includes long-lasting emotional attachment to the now-lost scam persona, which people grieve for."¹⁵⁶ If the next persona met online is sufficiently differentiated from the last, the victim may not recognize the new scam and choose to engage with the offender. Therefore, additional research into the effect of emotional loneliness on romance scam victimization may be valuable for identifying preventative measures aimed at initial and repeat romance scam victimization.

2. The Role of Attraction, Vividness, and Repetition in Belief Formation

Psychological and sociological literature is replete with studies into how people arrive at their decision to believe someone and comply with requests. Several of these lenses have already been applied to romance scams in other studies. In this section, I examine the effects that the profile picture, vivid stories, and repeated premises have on a victim's ability to judge truth. I propose these three concepts may increase a victim's likelihood of believing the offender.

I found frequent and adamant expressions of attraction to the persona's profile picture were common amongst the victims in this study. The frequency and intensity with which the victims express attraction supports the notion that physical attraction is an important consideration in the relationship for them. While attraction plays an obvious role in relationship formation, it may play a less obvious role in romance scams. Krueger, Vogrincic-Haselbacher, and Evans note that people use attractiveness as a cue for judging

¹⁵⁶ Sorell and Whitty, "Online Romance Scams and Victimhood," 348.

trustworthiness.¹⁵⁷ Thus, the attractive profile photo may prime individuals being targeted by romance scammers to believe the forthcoming premises by tapping into an unconscious tendency to believe people they find attractive.

Another aspect of the scheme that exploits a common error in judgement is the vividness of the premises. Examples of background stories offenders told victims in this study included being deployed military personnel in Afghanistan, working in the oil industry in Dubai, and owning a jewelry company in Poland. From the victim's engagement with these tales, I deduced that they found them compelling. Forgas and Baumeister, citing Kahneman and Tversky, report individuals "are more prone to believe interesting, captivating stories and narratives."¹⁵⁸ Therefore, like attraction, the vivid tales told by offenders may make victims more likely to believe them.

The last finding relevant to this section is the offender's persistent repetition of their premises. The "crafting and reasserting premises" code that captures this activity appeared in every case in the study. The literature on gullibility suggests that the offender's consistent repetition of their premises may play a role in the victim's acceptance of the offender's claims. Unkelbach and Koch report that the phenomenon of reiteration increasing the likelihood of belief is known as "repetition-induced truth."¹⁵⁹ A meta-analysis by Dechêne et al. demonstrates that repetition-induced truth is a widely studied and empirically valid psychological concept.¹⁶⁰ Therefore, repetition's prominent role in romance scams and empirical relationship with judging truth make it a likely candidate for playing a significant role in these scams.

Explanations for how repetition-induced truth functions have been sought for many years. Unkelbach and Koch propose a "referential theory of the repetition induced truth

¹⁵⁷ Joachim I. Krueger, Claudia Vogrincic-Haselbacher, and Anthony M. Evans, "Towards a Credible Theory of Gullibility," in *The Social Psychology of Gullibility: Fake News, Conspiracy Theories and Irrational Beliefs*, ed. Joseph P. Forgas and Roy F. Baumeister (New York, NY: Routledge, 2019), 115.

¹⁵⁸ Joseph P. Forgas and Roy F. Baumeister, "Homo Credulus: On the Social Psychology of Gullibility," in *The Social Psychology of Gullibility: Fake News, Conspiracy Theories and Irrational Beliefs*, ed. Joseph P. Forgas and Roy F. Baumeister (New York, NY: Routledge, 2019), 9.

¹⁵⁹ Unkelbach and Koch, "Gullible but Functional?," 43.

¹⁶⁰ Alice Dechêne et al., "The Truth About the Truth: A Meta-Analytic Review of the Truth Effect," *Personality and Social Psychology Review* 14, no. 2 (May 2010): 238–57, <https://doi.org/10.1177/1088868309352251>.

effect.”¹⁶¹ Their theory maintains that “correspondence and coherence” are necessary conditions for a person to judge information as true.¹⁶² They assert “correspondence” is how well “information” matches “with physical reality.”¹⁶³ Meanwhile, “coherence” refers to the logical links between different pieces of information. These links then form a network of references. According to the researchers, repeating the same information forms more links and increases the strength of belief. Thus, repetition is a key to belief formation.

“Processing fluency” is a crucial concept in referential theory according to Unkelbach and Koch that refers to the ease with which a person can process new information through the relevant network of related references.¹⁶⁴ When information is repeated, it increases the links between the corresponding references, allowing for more fluent processing of new information that activates those references. As a result, individuals can process information more quickly and confidently, leading them to perceive it as true or accurate, even if it is false or misleading.

Unkelbach and Koch’s referential theory thus posits that people judge the truth of a statement based on the number of coherently linked corresponding references it activates, as well as the fluency with which they process the statement.¹⁶⁵ As a result, people tend to believe incoming information that is coherent with their mental references and processed fluently, while they tend to disbelieve information that is incoherent or not processed fluently. Novel information that is not incoherent creates a new corresponding reference and is judged to be true, albeit weakly. As will be demonstrated, the concepts of coherence and fluency explain why victims may reject others’ attempts to point out the scam while rapidly judging exploitative requests from the offender as reasonable.

Take a relevant hypothetical example. Mindy meets Sam online. Because Sam is new to her, she creates a mental “Sam” reference and believes he is real. When Sam tells Mindy he works in the oil industry, she creates a link between her construct of “Sam” and

¹⁶¹ Unkelbach and Koch, “Gullible but Functional?,” 49.

¹⁶² Unkelbach and Koch, 49.

¹⁶³ Unkelbach and Koch, 55.

¹⁶⁴ Unkelbach and Koch, 51.

¹⁶⁵ Unkelbach and Koch, 48–52.

her mental references to the oil industry. Each time Sam repeats these claims, the links strengthen in Mindy's mind. Next, Sam claims he needs to travel to Dubai. Mindy likely already has a coherent link between her mental references between "Dubai" and "oil industry" so she finds the need for Sam to travel to Dubai to work in the oil industry coherent and judges it as true. Again, as these claims are repeated, the strength of the Mindy's network of relevant mental references increases and she processes related incoming information more fluently. Then, when Sam reports having an accident and needing money, Mindy's references for "foreign travel," "accident," "oil industry," and so forth make the new information coherent and thus believable. Of course, since Sam is a persona created by a romance scam offender, all of this information was false, resulting in a network of connections that have no correspondence with reality while being subjectively coherent to Mindy. Thus, by repeatedly receiving scheme-relevant information through consistent engagement with Sam, Mindy's ability to judge objective truth is degraded as it relates to Sam and his condition.

Research shows that repeated statements do not need to come from the same source to positively affect assessments of their truthfulness. Unkelbach and Koch report repetition-induced truth functions whether the same person repeats a claim or another person does.¹⁶⁶ This phenomenon may partially explain the use of other offenders in the guise of bankers, lawyers, or other characters in a scheme. The second offender's presentation of the same premise is another repetition, which may increase the likelihood of acceptance by the victim. As it relates to money mules, the use of the characters like a banker or lawyer may activate coherent references in the victim relating to money movement and helping. For instance, if the money mule has mental references that link a lawyer to helping people for money, then the money mule may find an offender's request to transfer money to a purported lawyer coherent.

This referential framework may provide insight into findings from past romance scam studies. For instance, Carter asserts that "the transformation from ordinarily unproblematic to apparently poor decision-making may not be due to the victim's over-romantic ideations (Lea et al. 2009a, Buchanan and Whitty 2013) but rather the skill of the

¹⁶⁶ Unkelbach and Koch, 45.

fraudster.”¹⁶⁷ Referential theory in this case might posit that the offender’s task is to provide scheme-relevant premises that link coherently to either mental references the victim already has or references the victim created through engagement with the offender. The offender’s skill then is how well they can advance coherent rather than incoherent premises.

Referential theory can also help explain how an individual can be both an unwitting romance scam victim and a witting money mule simultaneously. According to Unkelbach and Koch, “The localized nature of these networks also allows for conflicting beliefs within the same person.”¹⁶⁸ This phenomenon means that weakening the network of references regarding the transfer of money may not similarly weaken the references to the relationship. Thus, it may be subjectively coherent for the victim to believe they are in a relationship with the persona while disbelieving the reasons the persona gives for transferring incoming money.

The theory may also explain the slow adoption of belief when the money mule receives information from a banker or a police officer that they are participating in fraud. Because this information is incoherent with their mental references, it will be disbelieved. Information that is new but not incoherent will be judged as weakly true in the money mule’s mental references. This effect may explain the resilience romance scams exhibit with money mules and victims returning to offenders even after having received direct outside information refuting the genuineness of the relationship.

3. Proposed Definition of Grooming

Though numerous studies referred directly to the grooming of romance scam victims, no concise definition of grooming in the context of romance scams or online fraud was located. In this study, grooming is an offender’s repeated presentation of a series of false premises to a victim intended to exploit the victim’s inability to assess credibility effectively and to gain behavioral compliance with an exploitative request. For grooming

¹⁶⁷ Carter, “Distort, Extort, Deceive and Exploit,” 297.

¹⁶⁸ Unkelbach and Koch, “Gullible but Functional?,” 52.

to be successful in the study, victims had to accept enough premises for the offender's eventual request for money (i.e., theft) to appear reasonable.

Repetition of premises was present in all cases in this study. As previously noted, Unkelbach and Koch proposed a “referential theory” to explain repetition-induced truth.¹⁶⁹ The theory includes the creation of corresponding mental references that are coherently linked, allowing for fluent processing of information by an individual. By combining the observations in this study with the concepts in the referential theory, I derived a definition of grooming. Through these lenses, *grooming* is “an offender’s repeated presentation of scheme-relevant premises intended to create strong and coherently linked corresponding mental references in a victim, allowing for a victim to process future exploitative requests from the offender fluently.” This definition’s grounding in a generalizable theory of belief formation may make it transferable to other instances where repeated exposure to an idea or concept is the offender’s mechanism for building the victim’s worldview sufficiently that the victim accepts otherwise cognitively incoherent requests as valid.

The proposed definition also conforms to observations the researchers made about the potential intentional misuse of repetition. Unkelbach and Koch assert that if information is “strategically repeated,” it can lead to belief in a “falsehood.”¹⁷⁰ They point to propaganda as one type of strategic communication that can lead individuals to form beliefs that do not conform with normative assessments of reality. I propose grooming in the context of romance scams and money mules as another use case demonstrating the power of strategically employed repetition.

This definition of grooming can also be useful for the practitioner by setting the boundary conditions under which it occurs. Take, for example, the instances under the “Sending the Victim’s Own Money” code where victims voluntarily sent their money. The voluntary nature of the transfer could cast doubt on whether a crime occurred, since the offender made no explicit request for money.

¹⁶⁹ Unkelbach and Koch, 49.

¹⁷⁰ Unkelbach and Koch, 55.

However, understanding grooming as defined here aids in a deeper understanding of the fraud. There exists within the law the concept of an “artifice,” which is defined in the FindLaw Legal Dictionary as “a clever strategy usually intended to deceive or defraud.”¹⁷¹ Grooming can be understood as a type of artifice to defraud where the repetition of scheme-relevant premises results in the victim’s belief in the offender’s misrepresentations. An offender who receives money under the pretense of this artifice, then, has arguably defrauded the sender of the money through employment of the strategy of grooming.

4. Co-offending

From a review of the literature, this thesis may represent a first-of-its-kind look at the intersection of romance scams, money mules, and co-offending from the perspective of the victim’s progress through each stage. Though each of these concepts represents an emerging area of study, co-offending in fraud is particularly under-studied according to Free and Murphy.¹⁷² This thesis relies on two studies of co-offending to suggest explanations for phenomena that were encountered.

a. Co-offending and Affective Bonds

Co-offending from a witting money mule’s perspective is a dyad between romantic partners. Initially, the money mule believes they are helping their partner by transferring incoming money as directed. However, at some point the money mule receives outside information from banks or police about the money transfer. This feedback may occur rapidly enough that strong coherence has not yet formed around the offender’s premises supporting the money-transfer process. The offender’s premises may then begin to appear less true compared to the new incoming information. If the money mule continues to transfer incoming money after becoming aware of criminality, they transform into a witting, co-offending money mule.

¹⁷¹ FindLaw Legal Dictionary, s.v. “artifice,” accessed February 19, 2023, <https://dictionary.findlaw.com/definition/artifice.html>.

¹⁷² Free and Murphy, “The Ties That Bind,” 19.

Researchers have investigated the motives behind an individual's decision to co-offend. Free and Murphy identified three archetypes of co-offenders in their research of co-offending in fraud.¹⁷³ Of relevance to this study is the “affective bonds” archetype.¹⁷⁴ Free and Murphy demonstrated that the decision to co-offend for this archetype is based on a close, personal relationship with an offender rather than personal gains. They report that “the decision to co-offend is grounded in the affective desire for a relationship with another. As such, the decision to co-offend in this archetype was primarily a function of deep familial and friendship relationships; co-offending here was largely born out of psychological attachment to another.”¹⁷⁵ As was observed in this study, Free and Murphy note that co-offending “includes instances where participation in fraud was initially unwitting before a decision to continue to participate.”¹⁷⁶ Thus, they find that an emotional bond between co-offenders can serve as the basis for deciding to commit a crime even in an instance where there was no criminal intent for one of the co-offenders at the outset of the relationship.

The length of the relationship between the co-offenders may also play a role. It was noted in this study that the relationships between the money mules and offenders were not particularly new. As is demonstrated in Table 13, the relationships ranged between an estimated 17 and 30 months. This finding, too, is consistent with Free and Murphy's study, which reports that fraud perpetrated by co-offenders bonded by affective ties were characterized by long-standing relations.¹⁷⁷ The researchers explain that this is different than some other types of co-offending where the relationship is transient. So, co-offending based on intimate relationships is seen as having its own unique characteristics.

My findings appear to align with Free and Murphy's study. The money mule's motivation to co-offend is predicated on their romantic relationship with the persona, which

¹⁷³ Free and Murphy, 42.

¹⁷⁴ Free and Murphy, 40–42.

¹⁷⁵ Free and Murphy, 41.

¹⁷⁶ Free and Murphy, 19.

¹⁷⁷ Free and Murphy, 43.

is consistent with Free and Murphy’s “affective bonds” archetype.¹⁷⁸ Like the cases in Free and Murphy’s study, the individuals in this study likely used the relationship as “moral justification (helping friends or family)” for continuing to move money after recognizing criminality.¹⁷⁹ Therefore, it appears affective bonds may be the reason money mules who were victimized in romance scams choose to co-offend.

b. Personality and Co-offending

As stated earlier, my analysis suggests some victim characteristic may play a role in susceptibility to acting as a co-offender. I arrived at this conclusion based on the disparate outcomes different romance scam victims experienced while interacting with a single offender. A victim’s personality is one potential characteristic. Some researchers who study either romance scams or co-offending hypothesize that personality plays a role. Whitty, for instance, found personality variations during her study of romance scam victims.¹⁸⁰ Similarly, Ach Maulidi asserts that a researcher must take the offender’s traits into consideration when attempting to understand the motivation to commit fraud.¹⁸¹ Therefore, theorizing that personality may play a role in co-offending is supported by the literature as well as my data.

I attempted to falsify my theory that a co-offending money mule’s personality would differ from a romance scam victim’s by searching the literature for a personality trait that was strongly correlated with both outcomes. I was not able to locate one in my literature review. This finding lends support to my belief that there is a difference in a co-offending money mule’s personality compared to a romance scam victim’s. If there were a strong correlation in personality traits, one would expect more victims to have eventually become co-offending money mules.

¹⁷⁸ Free and Murphy, 32.

¹⁷⁹ Free and Murphy, 42.

¹⁸⁰ Whitty, “Do You Love Me?”

¹⁸¹ Ach Maulidi, “When and Why (Honest) People Commit Fraudulent Behaviours?: Extending the Fraud Triangle as a Predictor of Fraudulent Behaviours,” *Journal of Financial Crime* 27, no. 2 (January 13, 2020): 552, <https://doi.org/10.1108/JFC-05-2019-0058>.

However, since the co-offending money mules in my cases were first romance scam victims themselves, completely different personalities were not expected. This finding, too, was supported in the literature. The literature notes the personality trait “agreeableness” is present in co-offenders and romance scam victims, as well as online scam victims more generally.¹⁸² Kenethia McIntosh Fuller reported in her dissertation on personality traits and co-offending that agreeableness was correlated with co-offending.¹⁸³ Meanwhile, Modic and Lee’s study of online scam victimization generally revealed that agreeableness was among the personality traits that had “small to moderate correlations with response rates” but was not a “significant predictor” of scam compliance.¹⁸⁴ Whitty likewise found in her study of romance scam victims that some traits under the “agreeableness” dimension were predictive of victimization while others were not.¹⁸⁵ Therefore, I suggest that co-offending money mules may be more “agreeable” than other romance scam victims.

5. A Grounded Theory of the Evolution of Individuals into Co-offending Money Mules Through Engagement with Online Romance Scam Offenders

I now offer a grounded theory explaining how individuals become money mules after being victimized in online romance scams. The theory is firmly grounded in the data analyzed for this study. It is also heavily informed by relevant theories in the literature. The concept of “emotional loneliness” reported by Buecker et al. explains the motivation behind a person engaging with someone while seeking a romantic relationship.¹⁸⁶ Studies by McIntosh Fuller, Whitty, and Modic and Lee provide insight into personality traits that may make a person more vulnerable to co-offending and romance scams, respectively. This person is viewed as a “suitable victim” who meets an offender online according to Routine

¹⁸² Agreeableness is one dimension in the widely accepted and studied Five Factor Model of personality (FFM). According to McIntosh Fuller, “agreeableness is ascribed to ... caring, generous and trusting individuals” in the FFM. McIntosh Fuller, “Personality and Crime,” 1, 18.

¹⁸³ McIntosh Fuller, 159.

¹⁸⁴ David Modic and Stephen E. G. Lea, “How Neurotic Are Scam Victims, Really? The Big Five and Internet Scams,” *SSRN Electronic Journal*, 2012, 24, <https://doi.org/10.2139/ssrn.2448130>.

¹⁸⁵ Whitty, “Do You Love Me?,” 107.

¹⁸⁶ Buecker et al., “Loneliness and the Big Five Personality Traits.”

Activity Theory, as Pratt, Holtfreter, and Reisig have extended the concept to online interactions.¹⁸⁷

Concepts from Forgas and Baumeister and Krueger, Vogrincic-Haselbacher, and Evans explain how certain purported aspects of the persona may increase victim gullibility.¹⁸⁸ Alam's study using concepts drawn from Sternberg's Triangular Theory of Love sheds light on the language used in online relationship formation in romance scams.¹⁸⁹ Unkelbach and Koch's referential theory provides a framework to understand how victims form beliefs that do not match objective reality based on repeated interactions with an offender.¹⁹⁰ Referential theory also offers insight into how victims can recognize criminality relating to money laundering while still firmly believing they are in a genuine relationship with a scammer. Finally, Free and Murphy's study on co-offending provides context for a money mule's decision to co-offend.¹⁹¹ What follows is a grounded theory unifying my data with these studies and theories in the literature.

a. Grounded Theory

The scam begins when individuals experiencing emotional loneliness encounter a persona created by a motivated romance scammer on an online platform lacking safeguards to prevent victimization. Along with emotional loneliness, the victim possesses personality traits that may make them more individually prone to romance scams and co-offending. Through the offender's initial presentation of an attractive profile photo and vivid background stories, the intended victim is primed to believe the offender's future premises. The offender and victim exchange expressions of commitment, intimacy, and passion resulting in the formation of a romantic relationship.

Over time, the offender presents and repeats scheme-relevant premises designed to create strong and coherently linked corresponding references in the victim. The victim

¹⁸⁷ Pratt, Holtfreter, and Reisig, "Routine Online Activity and Internet Fraud Targeting."

¹⁸⁸ Forgas and Baumeister, "Homo Credulus: On the Social Psychology of Gullibility," 9; Krueger, Vogrincic-Haselbacher, and Evans, "Towards a Credible Theory of Gullibility," 115.

¹⁸⁹ Sternberg, "A Triangular Theory of Love"; Alam, "Three Essays on Socially Engineered Attacks."

¹⁹⁰ Unkelbach and Koch, "Gullible but Functional?"

¹⁹¹ Free and Murphy, "The Ties That Bind."

mentally codes the premises as weakly true when first exposed to them. However, each exposure to the premises creates additional links in the victim's mind, resulting in the victim increasingly believing the premises to be true. Next, the offender makes exploitative requests of the victim, which are coherent with the scheme-relevant premises. This coherence enables the victim to process the requests fluently, thus concluding that the requests are "true" or reasonable. Where the victim has the means and ability, they comply with these exploitative requests.

Certain types of exploitative requests related to acting as a money mule eventually result in the presentation of information from non-scheme sources like police and banks. The victim generally judges initial information from an outside source that is incoherent with the network they built through engagement with the persona as false and novel outside information as weakly true. However, repeated contact with the outside source causes the money mule to have increasingly strong coherence networks regarding the new information about the money. Eventually, the money mule judges the outside information regarding the money as true and the offender's statements about the money as less true.

During this process, not all coherence is lost between premises in the scam, because the coherence networks are localized. Therefore, the money mule continues to believe scheme-relevant premises related to the relationship and the persona's condition while disbelieving premises regarding the transfer of incoming money. Thus, there is no subjective incoherence between understanding they are participating in a crime and continuing in the relationship with the persona. Because they remain emotionally bonded to the offender, the money mule continues to comply with the exploitative requests related to acting as a money mule rather than risk losing the relationship and returning to their previous state of emotional loneliness. Thus, the individual has transformed into a co-offender who recognizes some criminal aspects of the money laundering scheme while still believing that the relationship with the persona is genuine.

b. Transferability

Because this theory is built on a robust data set and several generalizable theories, it may be transferable to other schemes. As articulated, the theory may be transferable to other cases where the scam is predicated on an offender grooming (as defined in this thesis)

an emotionally lonely person for exploitation. Likewise, the model should be transferable to offline variations of romance scams (e.g., loverboy scams in the Netherlands) since RAT is valid online and offline. Finally, if future research broadened the list of suitable victims and motivated offenders, the theory may be applicable to other fraud cases where grooming, as defined herein, occurs. Likely candidates include confidence scams, Ponzi schemes, work-from-home scams, and pyramid schemes.

D. LIMITATIONS

Though this study is based on a substantial data set, there were several limitations. It was clear from the data that offenders and victims communicated across many different platforms of which I had visibility into only one. Similarly, in some cases the relationship existed prior the offender and victim communicating via the platform I analyzed. Thus, not all communications were captured.

Because most of the study focused on historical cases, I was unable to interview the participants. This required me to rely on the communications as they were without the ability to ask clarifying questions. It also opens the possibility that communication I took as truthful on the part of the victim was not.

Finally, while the field interviews I conducted provided invaluable data for the study, none of the participants had acted as money mules. This inhibited me from directly interviewing a money mule about their lived experience. However, one victim did report that the scammer had introduced the concept of acting as a money mule to her, thereby allowing for first-hand input into the question of why all romance scam victims do not act as money mules.

E. RECOMMENDATIONS

As demonstrated by this thesis, romance scam victims who transform into money mules that later chose to co-offend is a multi-faceted, complex problem. With one exception, the recommendations I provide are relevant after the scam occurs. Naturally, this will be too late to avoid some victim damage. So, while prevention would be the preferred strategy, my study was not designed to produce data supporting the generation of preventative measures.

1. Romance Scam Warning Letter

This study mapped the process by which romance scam victims become money mules. In 11 of the cases, the offender introduced premises related to acting as a money mule.¹⁹² While only three complied, it does imply this is a relatively common tactic for money mule recruitment. Because it will not be possible to know initially if a romance scam victim is being groomed as a money mule, I recommend warning all romance scam victims of the possibility. I have attached a romance scam warning letter in Appendix C. It is intended for use by law enforcement, financial institutions, and others who may have contact with romance scam victims. It is intentionally written in a non-confrontational style to not engage mental defense mechanisms that might, paradoxically, nudge a victim closer to an offender, as Forgas and Baumeister report can happen when a person confronts “divergent views about reality.”¹⁹³

2. Persistent and Patient Engagement

The findings of this research and my personal experience working with this population suggest that disentangling a victim from a romance scam is a long process. As noted, the victim will have developed many mental links with the premises advanced by the offender. Referential theory posits that the longer the relationship lasted, the stronger these links will be. Therefore, persistent engagement with the victim may likely be necessary, since the new information about the scam will be perceived as less true.

Patience is also a must. While the scam references will be internally coherent to the victim, they will have no correspondence with reality for the person encountering the victim. This mismatch of world views can easily lead to frustration and victim-blaming on the part of the intended “helper.” However, it took time for the victim to build these mental references, so it will take time for them to build up other, more robust and truly correspondent networks.

¹⁹² Note: It is important to not generalize this recruitment rate to all romance scams. The cases in this study were selected for theoretical contribution not statistical purposes. Therefore, it would be an error to calculate an attempted rate of recruitment based on this study.

¹⁹³ Forgas and Baumeister, “Homo Credulus: On the Social Psychology of Gullibility,” 11.

3. Technological Solutions

As this thesis focused primarily on the psychological and criminological rather than technological aspects of online romance scams and related money mule schemes, I will not expound on what tech companies “should” do. I will point out that RAT proposes that the lack of a capable guardian is an essential ingredient for crime to occur. In this instance, the damage occurs once a victim begins to believe an offender. The longer the scam relationship continues, the greater the likelihood the victim will eventually suffer emotional, financial, and potential criminal consequences (should they wittingly act as a money mule). The only guaranteed way to stop this is to prevent the offender and victim from meeting. The scripted language the perpetrator employs, the stolen images delivered, the phone numbers used to target many victims, and involvement with an unusually high volume of users throughout the network are all potential candidates for technological targeting. Such technological approaches could reduce the risk of romance scam victimization and later co-offending.

4. Money Mule Investigations

Finally, this study has shown how offenders can groom victims to adopt internally coherent understandings of why they are receiving and sending money. Therefore, investigators must not jump to the conclusion that those who act as money mules in romance scams do so knowingly. However, this study also demonstrated that a person can simultaneously be a romance scam victim and a co-offending money mule. Thus, it is crucial that the investigator obtain copies of the communications via the appropriate legal process and then search for indicators that the money mule is aware they are participating in a crime by transferring money. Only by collecting appropriate communications can an investigator ascertain with certainty the money mule’s level of knowledge regarding their participation in criminal activity.

F. CONCLUSION

Romance scams are a pernicious problem. These scams enrich criminal organizations and are an arena from which to recruit people to assist with money laundering. It is difficult for police to investigate them due to a lack of cyber-investigations

skills, jurisdictional hurdles, and the time it takes to collect and analyze evidence. Additionally, romance scam victims can be challenging to deal with because they may have firmly adopted beliefs about the scammer having no basis in objective reality. These alternative viewpoints also make it easy to blame the victim. From this perspective, it is easy to comprehend why romance scams would go uninvestigated.

However, romance scams are a growing source of revenue for criminals. Beyond that, cybercrime provides an ever-larger dollar amount to criminal organizations. As demonstrated, money mules are essential in laundering the funds generated from these cybercrimes. Taking the time to disrupt a romance scam can have multiplicative effects. It can cut off that source of revenue for the criminal, stop the loss for the victim, eliminate a valuable node in a money laundering network, reduce the likelihood that the victim will later face criminal liability, and expose other members of a criminal conspiracy including money launders and potentially cyber criminals themselves. Preventing or disrupting romance scams is not only a means of protecting susceptible individuals but also plays a significant role in disrupting the criminal networks that profit from cybercrime and money laundering.

APPENDIX A. STUDY DOCUMENTS

A. EMAIL RECRUITMENT SCRIPT

Hello,

I am a master's degree candidate at the Naval Postgraduate School conducting a study that intends to describe how victims of online romance scams are sometimes convinced to send illegally obtained money on behalf of another person (i.e., act as a "money mule"). The research also seeks to explain why all romance scam victims do not act as money mules. The findings are meant to assist law enforcement, policymakers, and social media companies with detecting, investigating, and preventing these types of scams.

Anyone over the age of 18 who was the victim of an online romance scam is potentially eligible to participate in the study.

I will be interviewing 6 to 24 people. Based on your experience as a victim of a romance scam, I would greatly appreciate your participation in an interview. The interview can be conducted online, by phone, or at a place of your choosing such as your home or a quiet public location (e.g., a library). While I would ask that you set aside 2 hours for the interview, I will accommodate requests for longer or shorter timeframes. Participants will be asked to provide documents chronicling the scheme.

Participation in this study is confidential and voluntary. You may change your mind and decide not to participate at any time, even after the research has started. You may also choose to not provide any documents or limited documents. All participant information will be kept confidential. Interview data will be stored separately from personally identifiable information (e.g., your name) and linked with a coding key. Participant identities will be protected in reports through the use of pseudonyms. All records and data will be stored in secure facilities.

If you are interested in participating in this study, please contact me at christopher.huhn@nps.edu or 651-337-4537.

Regards,
Chris Huhn
christopher.huhn@nps.edu

The Principal Investigator, Dr. Kathryn Aten, may be contacted at 831-656-2644 or kjaten@nps.edu.

For questions about your rights as a research participant, contact Dr. Larry Shattuck: lgshattu@nps.edu

B. CONSENT FORM

Naval Postgraduate School Consent to Participate in Research

Introduction. You are invited to participate in a research study entitled “Love and Loss: A Multi-case Analysis of Romance Scam Victims and Their Role in Money Laundering Schemes.” The purpose of the research is to describe how individuals are convinced to send illegally obtained money on behalf of another person (i.e., act as a “money mule”) following victimization in online romance scams. The research also seeks to explain why all romance scam victims do not act as money mules.

- 1) Participation is voluntary. Refusal to participate will involve no penalty or loss of benefits to which you would otherwise be entitled, and you may discontinue participation at any time without penalty or loss of benefits to which you otherwise would be entitled.
- 2) Because this study is focused on romance scams, you will be asked about intimate details of romantic relationships. Some individuals may experience embarrassment, shame, or discomfort when discussing this topic. This study is also focused on “money mules,” which are people who transfer money on behalf of another person. Knowingly participating in money mule activity is potentially a crime. While all of your responses, including any potential admissions of guilt, will be kept confidential to the fullest extent of the law, the possibility exists that your answers could be disclosed in response to a subpoena or other legal process.
- 3) In contrast to #2, other people may find a sense of relief or resolution by talking through the events of their fraud. They may also derive some comfort by knowing their participation may reduce the chances of another person being victimized in the future. There is no direct benefit to you for participating in this study.
- 4) The alternative to participating in this study is to not participate.
- 5) Between 6 and 24 individuals will participate in an interview lasting approximately 2 hours. The interviews will take place online, by phone, at a public location, or at the participant’s home based on the participant’s preference. As a participant in this study, you will be asked to answer questions regarding your experiences as the victim of a romance scam, and if relevant, as a money mule. These questions are open-ended and intended to capture your unique experience as fully as possible. This interview will be audio-recorded and transcribed. The purpose of recording the interview is to ensure your answers to the questions are transcribed accurately. Recordings and transcriptions will be stored on a secure server at the Naval Postgraduate School. You will also be asked to provide documents relating to the scam such as emails, text messages, photos, and the like. You may choose to not answer individual questions, not provide documents, or withdraw from the study at any time.

Cost. There is no cost to participate in this research study.

Compensation for Participation. No tangible compensation will be given.

Confidentiality & Privacy Act. Any information that is obtained during this study will be kept confidential to the full extent permitted by law. All efforts, within reason, will be made

to keep your personal information in your research record confidential but total confidentiality cannot be guaranteed. This consent form will be converted to a digital format and the original will be destroyed. You will be provided a copy of this consent form at your request. As soon as possible after this interview, the interview of the recording and the transcription will be downloaded to a secured server at the Naval Postgraduate School. Your personally identifiable information (e.g., name) will be separated from the interview data and linked by a coding key. That key will be stored separately. Only the researchers will have access to the records and data. However, it is possible that the researcher may be required to divulge information obtained in the course of this research in response to a lawfully issued subpoena or order of a court with competent jurisdiction. Only the data specifically described in a subpoena or court order will be disclosed. Your anonymized data could be used for future research studies or distributed to another investigator for future research studies without additional informed consent.

If you consent to be identified by name in this study, any reference to or quote by you will be published in the final research finding only after your review and approval. If you do not agree, then you will be identified broadly by discipline and/or rank, (for example, “fire chief”).

- ☐ I consent to be identified by name in this research study.
- ☐ I do not consent to be identified by name in this research study.

Points of Contact. If you have any questions or comments about the research, or you experience an injury or have questions about any discomforts that you experience while taking part in this study please contact the Principal Investigator, Dr. Kathryn Aten, 831–656-2644, kjaten@nps.edu. Questions about your rights as a research subject or any other concerns may be addressed to the Navy Postgraduate School IRB Chair, Dr. Larry Shattuck, 831–656-2473, lgshattu@nps.edu.

Additional assistance is available to you from your county’s social services agency or your local law enforcement agency. The American Association of Retired Persons also provides assistance with scams. They can be contacted at 877–908-3360.

Statement of Consent. I have read the information provided above. I have been given the opportunity to ask questions and all the questions have been answered to my satisfaction. I have been provided a copy of this form for my records and I agree to participate in this study. I understand that by agreeing to participate in this research and signing this form, I do not waive any of my legal rights.

- ☐ I consent to participate in the research study.
- ☐ I do not consent to participate in the research study.

Signature of Participant

Date

C. INTRODUCTORY SCRIPT

My name is Chris Huhn, and I am pursuing a master's degree at the Center for Homeland Defense and Security in Monterey, CA. I have an interest in romance scams and money laundering that developed from working with victims of these schemes. The purpose of this interview is to explore and describe how suspects scam victims out of money through fake online romantic relationships. Another aspect of the study is understanding how these same suspects sometimes convince victims to transfer other people's money for the suspect. I want to understand the experiences of people who have been targeted by romance scams. I am interested in your story in whatever manner or order you would like to tell it. I have questions to guide our conversation, but please feel free to tell your story or add details as they come to you. My hope is the study will uncover methods that can be used to reduce these types of crimes.

Before we begin, you will be asked to review and sign a consent form. You may ask me any questions before signing the form. Participation in this study is completely voluntary. Even after signing the consent form, you may choose to withdraw from the study by asking to end the interview at any time. You may also choose to not answer particular questions or provide documents.

Because money laundering is one of the topics of the research, you should be aware that any statements you make to me may include admissions of guilt on your part. That is, you may be speaking about, or providing documents of, a crime that you were knowingly or unknowingly a part of. All of your answers to my questions will be kept confidential to the fullest extent of the law. They will not be reported to law enforcement, nor will they be used to launch an investigation. However, confidentiality cannot be absolutely assured. In some rare instances, such as the issuance of a subpoena or other legal order, I may be compelled to produce copies of this interview and related documents. I am attempting to reduce this risk to you by keeping your participation in the study confidential, storing the interview and transcription on a secure server at the Naval Postgraduate School, and removing all of your identifiers from the records prior to publishing the study. Only the principal investigator and I will have access to the key code that links your identity to the interview or records you provide today.

Do you have any questions for me before we review the consent form?

D. INTERVIEW QUESTIONS

Were you defrauded (i.e., lost money, property, or something of value) by a person you had romantic relationship with online?

Did this person ever ask you to receive money, property, or another item of value on their behalf and send it to them or another person?

Please tell me the story of how you came to seek an online relationship? What led you to decision to look online? What steps did you take to find a dating site?

Possible Probes:

- Why did you decide to seek a relationship online?
- How did you find a site?
- What sites/venues did you consider?

Please tell me how you eventually connected with a dating partner? Begin with how he or she came to your attention and tell me about the steps that led to connecting?

Possible Probes:

- What attracted you to [name]?
- How did you initially communicate with [name]?
- Explain how your communications evolved or did not over time (i.e., did you use different platforms or methods)?
- How did you feel about the communication?

(Early days) Tell me the story of how your relationship developed and progressed beginning with getting to know [name]?

Possible Probes:

- How did you come to know each other?
- What were some of the key turning points or memorable events in the early days of your relationship?
- How did your trust in [name] develop? What did [name] do that led you to trust him/her?
- During the early days, how did your trust in this person compare with other relationships in your life?

(Mid days) Tell me how [name] first asked you for money? How did you feel about the request?

Possible Probes:

- What reasons did [name] give you for needing the money?

- What about the reasons were compelling?
- How did [name] alleviate any fears or suspicions you had about the relationship or the requests they made of you?
- What, if any, hardships or difficulties did you experience in complying with these requests?

Tell me about any bank accounts you opened at [name's] request or credit cards or loans you obtained?

Possible Probes:

- Why did these requests seem reasonable?
- What did [name] say [he/she] was going to do with this money?
- How did [name] with reassurances that you would be repaid or that it was worth it to you to send the money?

Tell me how [name] first asked to receive money from someone else and forward it? How did you feel about the request?

Possible Probes:

- What reasons did [name] give you for not being able to receive the money [himself/herself]?
- What about the reasons were compelling?
- How did [name] alleviate any fears or suspicions you had about conducting the transactions?
- How did [name] know [he/she] could trust you with this money?
- What sort of proof, if any, did [name] ask for to show you were correctly receiving and sending the money?
- Note: for romance scam victims who were not money mules, these questions will be asked hypothetically (e.g., "If [name] asked, would you have received money from someone else and forwarded it?")

Tell me about any business you created or that were established in your name at [name's] request.

Possible Probes:

- What reasons did [name] give you for establishing these businesses?
- What made these reasons believable to you?

(Key Events) All relationships have rough spots. Can you tell me about a time you had an argument or questioned the relationship?

Possible Probes:

- What lead to the argument(s)?
- How did [name] address your concerns?

- If [name] was upset with you, what triggered that?
- What did you most frequently argue over and why?

Tell me about any communications you had with this person's friends, colleagues, or assistants. Did they make any requests of you?

Possible Probes:

- How did communication with these people affect your perception of your relationship with [name]?
- What additional requests did these people make of you?
- How did you feel about these requests?
- How did they alleviate any of your concerns about these requests?

(Outcomes) Tell me about a time someone like a friend, bank employee, or the police tried to convince you the relationship was a scam?

Possible Probes:

- Tell me about any conversations you had with [name] where you brought up this other person's concerns. How did [name] react?
- Why did you choose to trust [name] over the person who was warning you?
- What requests or demands did [name] make of you in regards to this person?

How did you come to realize you were being scammed?

Possible Probes:

- What effect did public awareness campaigns about romance scams, money mules, or online fraud have on you?
- Reflecting back, how could you have become aware you were being victimized earlier or avoided the scam altogether?

What led you to no longer being involved in moving money for [name]?

Possible Probes:

- Who was the most influential in getting you to stop sending money and why?
- What led you to trust this other person over [name]?

What effect did this relationship have on other relationships in your life?

Possible Probes:

- How has this experience shaped your attitude towards online relationships?
- How has this experience shaped your attitude towards offline relationships?
- How has your current relationship been affected by the scam?

Tell me about your experiences sharing your story with others such as bank employees, friends, family, or law enforcement after you realized you had been scammed.

Possible Probes:

- In what ways were these individuals helpful or not?
- How did these individuals show you (or not show you) they were understanding of your experience?

E. POST-SCRIPT

Thank you for your time and participation in this study. If you wish, I will send you a transcription of this interview by U.S. mail or email. Bear in mind that having a copy of the transcription increases the likelihood that someone other than you, the principal investigator, and I become aware of your participation in the study.

The study will be publicly available on the internet sometime after March 2023. Simply conduct a search for “CHDS Thesis” and then search by author for “Huhn.”

If you have questions, concerns, or additional information you would like to provide in the future, please contact me at christopher.huhn@nps.edu.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX B. ROMANCE SCAM SCRIPTS

#	Script	Victim	Victim Response
1	Baby i am the only child of my parents. i lost my parents late last year, i really do not have a big family as such	AV1.3	OK do you like me
		AV1.4	My parents are gone also but I have four sisters and two grandchildren
		AV1.21	<i>Missed Call</i>
2	You are my ultimate secret keeper. Thank you for trusting me. Thank you treating me respectfully at all times. Thank you for being vulnerable and open to me. I know as a man that can be very difficult to do, but it's developed a closeness that I value each moment I spend with you. Thank you for being the kind of man who does all of these things without a second thought.	AV1.1	Baby you are very welcome. I love you too. Kisses back.
		AV1.21	<i>Missed Call</i>
3	Good Morning sunshine how was your night when you imagine days full of affection and nights full of passion, when you dream of full harmony and happiness, know that I share your thoughts, because your dreams are my best dreams, and my greatest wish is to see you always well and happy! I love you. Perhaps it would even be unnecessary to say this, as I believe that my feelings are evident in each of my gestures and in every word that I speak. That is why I dare to say that your dreams are ours and, therefore, in not too distant days they will become reality. Love has this fantastic power to transform noble and generous ideas into fact. Love is miraculous because it adds virtues and makes the world and people better. Love is sacred because it brings us closer to the beautiful and the perfect. And it is this love, fantastic, miraculous and sacred, that I feel for you. It is this love that makes me believe, without a doubt, that your dreams are mine too. I'm happy to have you by my side. I am happy to still be able to believe in dreams in this world so skeptical of everything. I am happy because I am fortunate to have your company, it's that company that leads me to believe that the next day will always be better than the current or the previous one. Dream, my love. Dream a lot. I will always be by your side, whether you are sleeping or even, and especially, when you wake up.	AV1.1	Good morning mommy daddy loves you.
		AV1.2	He gets held and I just get to see how beautiful you are and how pretty he gets your attention now but I'm here

#	Script	Victim	Victim Response
4	Well I should start this way ...Am the only child of my flock,I was born in Louisville Kentucky and my dad was a business man and at the same time a bridge architecture,my mom was a trader and she own a whole lot of supermarkets before ...My dad was a traveler he never had time for the family his always consigned about his work and his attorney.. he would choose his attorney over any of the family members,,then the trouble all started when my mom though my dad was married to another woman because he his always out of the house ..my mom met a man then and they started talking and before we could know what's going on mom already used her supermarkets to collect loan for this damn Guy !! And we loosing mom properties already ..When my dad found out about it he started keeping whole lot of things from us and he only gave us another house in Texas and he told us about him having a shoe factory in CAD when the whole issues was already settled and we all thought our family was back to normal and that everything was okay for us already.....We we're a happy family all again but still my dad didn't open up to us finally and some years back about 4years now my dad died and everything rumbled most of our landed properties were seized to tax enforcement our house in Texas was used to collect a loan but we haven't lost it still ...	AV2.1	I guess we really do have a lot in common I just love you
		AV2.4	No you didn't scare me off I am so glad you shared that with me and of course I will be praying for you to be able to get your dad money back
		AV2.15	Wow baby I will keep you in my prayers always
5	Every morning when I wake up the first thing hit my mind, is you. I close my eyes and picture your beautiful face in my head so I can start the day full of positivity. I feel lucky to have you in my life. You are a blessing that I will be thankful to God for the rest of my life	AV2.1	I was just thinking about you
		AV2.7	Hi I left you a message on POF. Read it when you get the chance. For now that's how I want to communicate with you .I'm only texting you so you know I did write you back.
6	I never thought of falling in love with someone I barely knew. Then suddenly I met you one day and something in my ear whispered that this is the girl that I have ever wanted in my life. Since then, all I know is that I love you and want to be with you forever.	AV2.1	I love you so much
		AV2.4	Thank you so much sweetheart for tell me that. I feel the same way about you I want to spend

#	Script	Victim	Victim Response
			the rest of my life with you and you only I am very rueful person. I have been hurt so many times before for. But there is something special about you that I feel in love with so very quickly. Love you so very much sweetheart
		AV2.4	Honey I want you and only you for the rest of my life. IOVE YOU SO VERY MUCH
		AV2.7	AS2.1[v2] what happened to baby steps. All of that is to much. It's overwhelming these feelings you seem to have for me I just need you to dial it back for me. Ok
		AV2.7	Well you think you know me so well.. throwing a guilt trip at me. Your wrong on so many levels. I really shouldn't have to explain myself to you but since this is the last time we'll be texting here it is...Your right I haven't texted you but it's because you keep throwing these I love yous at me when I asked you numerous times to pull back. You dont know me you haven't even

#	Script	Victim	Victim Response
			spoke to me on the phone never met in person so I find it a little bit to much. Since when I asked you to stop and you didn't listen I did the only thing I could. I chose to step back. We want different things you want a wife I'm not ready for that you want me to leave everything I have here to be with you and how can I do that when I barely know you. I truly hope you find what your looking for AS2.1[v2] I'm sorry it wasn't me. Please be safe and goodbye.
		AV2.15	Baby...Bye...Because I found that the military guys on pof just want women to help get passes or other items
7	That moment I fell in love with you, you didn't just steal my heart away, you also went away with the remote control of my life, honestly, you have taken control over me, and I am settled because my life is in perfect hands, I love you every day of my life	AV2.16	OH MY PERFECTLY SAID I. DONT KNOW WHAT 2 SAY I JUST DONT KNOW UGOOD ENOUGH 2 SAY THE SAME 2 U I DONT SEE HOW U COULD FEEL THAT WAY NOT KNOWING SOMEONE PLEASE DONT TAKE WHAT I SAID WRONG IT WOULD B ALOT

#	Script	Victim	Victim Response
			EASIER TALKING 2 U ON THE PHONE
		AV2.19	Baby I'm here sorry I don't feel very good.
		AV2.19	I haven't heard from that from a long time.
8	I think we are Looking for the same things but mine in a Woman, Just that i am Looking for a nice, Honest, Kind and Caring Woman, a Woman that will Love and be with me for the Rest of my Life.... Am not looking for someone to date but someone to spend the rest of my life with, All i need from you is just being sincere to me,make me feel secured,appreciate,love,care and being understanding, All my life has been engulfed with misery and loneliness,i watch my life layed wide spread in front of me and didn't know what to do with it,my life has been so boring and hope with someone who is ready to Love me for who i am now it's gonna change for the best	AV2.4	We are looking for the same thing
		AV2.15	My life hasn't been all bad I think of others and I think I could always be worse I have had a few shiity men but I know there is a soulmate for everyone so I keep hoping I will find mr right some day
		AV2.16	WOW U SAID THAT PERFECT WE WANT THE SAME I HAD ALOT OF BAD GUYS IN MY LIFE I DID DRUGS 4 A LONG TIME I HAVE BEEN CLEAN AN SOBER 4 8YRS THAT PART OF MY LIFE IS OVER I HAVE NO DESIRE ANYMORE 4 THAT

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX C. ROMANCE SCAM WARNING LETTER

This study found that romance scams are a common vector for money mule recruitment. Because it will not be possible to know initially if an offender is actively grooming a romance scam victim to be a money mule, I recommend warning all romance scam victims of the possibility. The following romance scam warning is intended for use by law enforcement, financial institutions, and others who may have contact with romance scam victims. It is intentionally written in a non-confrontational style to encourage recognition of the scam and discourage acting as a money mule.

Date:

Dear [INSERT NAME]:

It is likely that you will want to dismiss or ignore this letter. Please do not because we have important information to share with you. We believe you have been the victim of a romance scam. It may be helpful for you to write down some of the doubts you have had about the relationship before reading this entire letter. Some of the common warning signs of a romance scam are online relationships that quickly progressed to expressions of love and commitment, promises to meet that are broken, claims of a large inheritance, travel to another state or a foreign country where an emergency is encountered, reporting difficulties transferring money due to “frozen” accounts, and requests for money to help the person out of an emergency. This is not a complete list. Many variations of the scam exist.

Often, people do see several warning signs or “red flags” during these relationships. People commonly ignore them for a variety of reasons. It is important you no longer ignore the signs you have seen. A technique you can use is to search for some of the photos the person sent you using a “reverse image search.” These photos are almost always stolen from other victims. You can also search the internet to see if the long stories, poetry, and other love stories were scripts that the person reused. There is little point in confronting the person you are messaging with your concerns and findings. They will have a story prepared designed to reassure you.

Please know that you are at further risk of being a victim. It is common for people to be approached online by another romance scammer. Another variation is for a scammer posing as a government official to offer to help you recover money you lost for a fee. To avoid scams in the future, it is important for you to identify the underlying reasons you were victimized and find a way to address those issues, so it does not happen again.

Finally, some scammers ask romance scam victims to transfer money for them. The scammer then has money sent to the victim and asks the victim to forward that money. Victims who comply with these requests are actually helping the scammer launder money from other victims. The term for individuals who do this is “money mules.” It is important you do not transfer money from other parties, as you could be charged with a crime if you participate knowingly. If you have been in a long-term relationship with the scammer, you may be tempted to transfer money at their request to maintain the relationship out of a misplaced sense of loyalty and “just in case it’s real.” This is not a genuine relationship. A look at your bank account will show you the money is only going one way.

We ask that you file a report of your experience with the Internet Crime Complaint Center website found at www.ic3.gov. Doing so may help law enforcement identify the scammer and prevent him or her from harming others.

APPENDIX D. ADDITIONAL DATA TABLES

Table 17. Presence of Codes in the “Grooming the Victim” Dimension

1st Order Codes	Quotes Supporting Code Present																						
	Archival Case 1										Archival Case 2										In-Person Cases		
	2	3	4	5	6	7	8	9	21	2	3	4	7	8	9	10	15	16	19	1	2.1	2.2	3
<i>Persona Identity and Biography</i>	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
<i>Persona Past and Present Location</i>	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
<i>Baseline Financial Status</i>	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	Y	Y	Y	Y	N	Y	Y	Y	Y
<i>Commitment</i>	Y	Y	Y	Y	Y	N	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
<i>Passion</i>	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	Y	Y	Y	Y	Y	Y	Y	N	Y	Y	Y	Y
<i>Intimacy</i>	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
<i>Dissatisfaction</i>	Y	Y	N	Y	Y	N	N	N	N	Y	Y	N	Y	Y	N	Y	Y	Y	N	Y	Y	Y	N
<i>Crafting and Reasserting Premises</i>	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
<i>Providing Characters and Objects</i>	Y	Y	N	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
<i>Manipulating Moods</i>	Y	Y	Y	Y	Y	Y	Y	Y	N	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	Y	Y	Y	Y
<i>Explaining Away Inconsistencies</i>	Y	Y	Y	Y	Y	Y	Y	N	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y

Table 18. Presence of Codes in the “Exploiting the Victim or Money Mule” Dimension

1st Order Codes	Quotes Supporting Code Present																						
	Archival Case 1										Archival Case 2										In-Person Cases		
	2	3	4	5	6	7	8	9	21	2	3	4	7	8	9	10	15	16	19	1	2.1	2.2	3
<i>Gathering Personal Information</i>	Y	Y	Y	Y	N	Y	Y	Y	Y	Y	N	Y	Y	Y	N	Y	Y	Y	N	Y	N	Y	N
<i>Requesting Items of Value</i>	Y	Y	Y	N	Y	N	Y	Y	N	Y	Y	Y	Y	Y	Y	Y	N	Y	Y	Y	Y	Y	Y
<i>Persuading</i>	Y	Y	Y	Y	Y	N	Y	Y	N	Y	Y	Y	Y	Y	Y	Y	N	Y	Y	Y	Y	Y	Y
<i>Preparing for the Movement of Money</i>	N	Y	N	Y	N	Y	Y	Y	N	N	N	Y	N	N	N	N	N	N	N	N	N	Y	Y
<i>Directing the Movement of Money</i>	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N
<i>Coaching</i>	N	N	N	N	N	N	N	Y	N	Y	Y	Y	N	N	N	N	N	Y	Y	Y	N	Y	N
<i>Collaborating</i>	N	N	N	N	N	N	N	N	N	N	N	Y	N	N	N	N	N	N	N	Y	N	N	N

Table 19. Presence of Codes in the “Engaging the Persona” Dimension

1st Order Codes	Quotes Supporting Code Present																						
	Archival Case 1										Archival Case 2										In-Person Cases		
	2	3	4	5	6	7	8	9	21	2	3	4	7	8	9	10	15	16	19	1	2.1	2.2	3
<i>Death</i>	N	N	N	N	N	N	N	N	N	N	N	Y	N	N	Y	Y	N	N	Y	Y	Y	Y	N
<i>Divorce</i>	Y	N	Y	N	N	N	N	N	N	N	N	N	Y	N	N	N	N	N	N	N	N	N	Y
<i>Illness</i>	Y	N	Y	N	N	N	N	N	N	N	N	Y	N	N	N	N	N	N	Y	N	N	N	N
<i>Non-specific Origin</i>	Y	N	Y	Y	N	N	N	N	N	N	N	N	N	Y	N	N	Y	N	N	Y	Y	Y	Y
<i>Commitment</i>	Y	Y	Y	N	Y	N	N	Y	Y	Y	Y	Y	N	N	N	N	N	N	Y	Y	Y	Y	Y
<i>Passion</i>	Y	Y	Y	Y	Y	Y	Y	N	N	Y	Y	N	Y	Y	Y	Y	Y	N	N	Y	Y	Y	Y
<i>Intimacy</i>	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
<i>Dissatisfaction</i>	Y	N	Y	Y	Y	N	N	Y	Y	Y	Y	Y	Y	Y	N	Y	Y	Y	N	Y	N	Y	N

<i>Accepting Premises</i>	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
<i>Questioning or Rejecting Premises</i>	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
<i>Receiving Outside Information</i>	Y	Y	Y	N	Y	N	Y	N	N	Y	N	Y	Y	N	N	N	Y	N	Y	Y	Y	Y	Y
<i>Acknowledging Criminality</i>	Y	N	N	N	Y	N	N	N	Y	N	N	Y	N	N	N	Y	N	Y	N	Y	Y	Y	Y

Table 20. Presence of Codes in the “Assisting the Persona” Dimension

1st Order Codes	Quotes Supporting Code Present																						
	Archival Case 1									Archival Case 2										In-Person Cases			
	2	3	4	5	6	7	8	9	21	2	3	4	7	8	9	10	15	16	19	1	2.1	2.2	3
<i>Providing Personal Information</i>	Y	Y	Y	Y	N	Y	N	Y	Y	N	N	Y	Y	Y	N	Y	Y	Y	N	Y	N	Y	N
<i>Sending the Victim’s Own Money</i>	Y	N	N	N	Y	N	N	N	N	N	Y	Y	N	N	N	N	N	Y	N	Y	Y	Y	Y
<i>Expresses a Lack of Means</i>	Y	Y	Y	N	N	Y	Y	Y	N	Y	Y	Y	N	Y	Y	Y	N	Y	N	N	N	N	N
<i>Expresses a Lack of Ability</i>	N	N	N	N	N	N	N	N	N	N	Y	N	N	N	N	N	N	Y	Y	N	N	Y	N
<i>Coordinating the Transfer of Incoming Money</i>	N	Y	N	Y	Y	N	N	Y	N	N	N	Y	N	N	N	N	N	N	N	N	N	N	N
<i>Transferring Incoming</i>	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N

1st Order Codes	Quotes Supporting Code Present																						
	Archival Case 1										Archival Case 2										In-Person Cases		
	2	3	4	5	6	7	8	9	21	2	3	4	7	8	9	10	15	16	19	1	2.1	2.2	3
<i>Money as Directed</i>																							
<i>Increasing Knowledge and Capabilities</i>	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	Y	N
<i>Collaborating</i>	N	N	N	N	N	N	N	N	N	N	N	Y	N	N	N	N	N	N	N	Y	N	Y	N
<i>Persevering</i>	N	N	N	N	N	N	N	N	N	Y	Y	Y	N	N	N	N	N	N	N	Y	N	N	N

Table 21. Estimated Length of Money Mule Relationships

Label	First Text	Last Text	Quote	Estimate
AV1.1	March 2020	December 2020	“Baby this as been going on for over a year now,” (AV1.1 to AS1, May 2020).	19 months
AV2.1	August 2018	February 2020	AS2, “Are you getting my text?” AV2.1, “I am. I miss talking to you.” (AS2 and AV2.1, September 2018).	17 months
AV3	November 2016	December 2016	“I can’t remember is two and a half years ago,” (Transcript of Police Interview of AV3, August 2017).	30 months

LIST OF REFERENCES

- Adejoh, Samuel O., Tunde A. Alabi, Waziri B. Adisa, and Nnenna M. Emezio. “‘Yahoo Boys’ Phenomenon in Lagos Metropolis: A Qualitative Investigation.” *International Journal of Cyber Criminology* 13, no. 1 (June 2019). <https://doi.org/10.5281/ZENODO.3366298>.
- Africa Eye. “The Ultra-Violent Cult That Became a Global Mafia.” BBC News, December 13, 2021. <https://www.bbc.com/news/world-africa-59614595>.
- Agari Cyber Intelligence Division. *The Geography of BEC: The Global Reach of the World’s Top Cyber Threat*. Threat Intelligence Brief. Foster City, CA: Agari Data, 2020. <https://www.agari.com/cyber-intelligence-research/whitepapers/acid-agari-geography-of-bec.pdf>.
- Alam, Md Nabid. “Three Essays on Socially Engineered Attacks: The Case of Online Romantic Scams.” PhD diss., University of North Carolina at Greensboro, 2021.
- Al-Rousan, Suhaib, Abdullah Abuhussein, Faisal Alsubaei, Ozkan Kahveci, Hazem Farra, and Sajjan Shiva. “Social-Guard: Detecting Scammers in Online Dating.” In *2020 IEEE International Conference on Electro Information Technology (EIT)*, 416–22. Chicago, IL, USA: IEEE, 2020. <https://doi.org/10.1109/EIT48999.2020.9208268>.
- “Anti-Money Laundering Regulations for Dealers in Antiquities.” Federal Register, September 24, 2021. <https://www.govinfo.gov/content/pkg/FR-2021-09-24/pdf/2021-20731.pdf>.
- Barnor, Jonathan Nii Barnor, Richard Boateng, Emmanuel Awuni Kolog, and Anthony Afful-Dadzie. “Rationalizing Online Romance Fraud: In the Eyes of the Offender.” *AMCIS 2020 Proceedings* 21: 12. Accessed March 5, 2022. https://www.researchgate.net/profile/Emmanuel-Kolog/publication/343392445_Rationalizing_Online_Romance_Fraud_In_the_Eyes_of_the_Offender/links/5f31381092851cd302ec0508/Rationalizing-Online-Romance-Fraud-In-the-Eyes-of-the-Offender.pdf.
- Better Business Bureau. “Fall in Love, Go to Jail: BBB Report on How Some Romance Fraud Victims Become Money Mules.” Latest News, February 15, 2019. <https://www.bbb.org/article/news-releases/19398-fall-in-love-go-to-jail-bbb-report-on-how-some-romance-fraud-victims-become-money-mules>.
- Boeri, Miriam, and Aukje K. Lamonica. “Collecting and Interpreting Qualitative Data.” In *The Routledge Handbook of Qualitative Criminology*, edited by Heith Copes and J. Mitchell Miller. New York, NY: Routledge, 2015.

- Bryant, Antony, and Kathy Charmaz. *The SAGE Handbook of Grounded Theory*. Los Angeles: SAGE, 2007.
- “BSA Timeline | FinCEN.Gov.” Accessed November 20, 2021. <https://www.fincen.gov/resources/statutes-regulations/bank-secrecy-act/bsa-timeline>.
- Buchanan, Tom, and Monica T. Whitty. “The Online Dating Romance Scam: Causes and Consequences of Victimhood.” *Psychology, Crime & Law* 20, no. 3 (March 16, 2014): 261–83. <https://doi.org/10.1080/1068316X.2013.772180>.
- Buecker, Susanne, Marlies Maes, Jaap J. A. Denissen, and Maike Luhmann. “Loneliness and the Big Five Personality Traits: A Meta-Analysis.” *European Journal of Personality* 34, no. 1 (January 2020): 8–28. <https://doi.org/10.1002/per.2229>.
- Buil-Gil, David, and Yongyu Zeng. “Meeting You Was a Fake: Investigating the Increase in Romance Fraud During Covid-19.” *Journal of Financial Crime*, May 10, 2021. <https://doi.org/10.1108/JFC-02-2021-0042>.
- Carter, Elisabeth. “Distort, Extort, Deceive and Exploit: Exploring the Inner Workings of a Romance Fraud.” *The British Journal of Criminology* 61, no. 2 (February 26, 2021): 283–302. <https://doi.org/10.1093/bjc/azaa072>.
- Chua, Yi Ting, Simon Parkin, Matthew Edwards, Daniela Oliveira, Stefan Schiffner, Gareth Tyson, and Alice Hutchings. “Identifying Unintended Harms of Cybersecurity Countermeasures.” In *2019 APWG Symposium on Electronic Crime Research (ECrime)*, 1–15. Pittsburgh, PA: IEEE, 2019. <https://doi.org/10.1109/eCrime47957.2019.9037589>.
- Corbin, Juliet M., and Anselm L. Strauss. *Basics of Qualitative Research: Techniques and Procedures for Developing Grounded Theory*. 3rd ed. Los Angeles: SAGE, 2008.
- Cross, Cassandra. “‘Oh We Can’t Actually Do Anything About That’: The Problematic Nature of Jurisdiction for Online Fraud Victims.” *Criminology & Criminal Justice* 20, no. 3 (July 2020): 358–75. <https://doi.org/10.1177/1748895819835910>.
- Cross, Cassandra, and Michael Kelly. “The Problem of ‘White Noise’: Examining Current Prevention Approaches to Online Fraud.” *Journal of Financial Crime* 23, no. 4 (October 3, 2016): 806–18. <https://doi.org/10.1108/JFC-12-2015-0069>.
- Cross, Cassandra, and Rebecca Layt. “‘I Suspect That the Pictures Are Stolen’: Romance Fraud, Identity Crime, and Responding to Suspicions of Inauthentic Identities.” *Social Science Computer Review*, March 2021. <https://doi.org/10.1177/0894439321999311>.

- Cross, Cassandra, Molly Dragiewicz, and Kelly Richards. "Understanding Romance Fraud: Insights from Domestic Violence Research." *The British Journal of Criminology* 58, no. 6 (October 5, 2018): 1303–22. <https://doi.org/10.1093/bjc/azy005>.
- Customer identification program requirements for banks, 31 CFR § 1020.220. Accessed November 20, 2021. <https://www.law.cornell.edu/cfr/text/31/1020.220>.
- Dechêne, Alice, Christoph Stahl, Jochim Hansen, and Michaela Wänke. "The Truth About the Truth: A Meta-Analytic Review of the Truth Effect." *Personality and Social Psychology Review* 14, no. 2 (May 2010): 238–57. <https://doi.org/10.1177/1088868309352251>.
- Department of Justice. "U.S. Law Enforcement Takes Action Against Approximately 2,300 Money Mules In Global Crackdown On Money Laundering." Justice News, December 2, 2020. <https://www.justice.gov/opa/pr/us-law-enforcement-takes-action-against-approximately-2300-money-mules-global-crackdown-money>.
- Diaz, Sara Katherine. "Where Do I Start? Decision Making in Complex Novel Environments." Master's thesis, Naval Postgraduate School, 2010. <http://hdl.handle.net/10945/5132>.
- Esoimeme, Ehi Eric. "Identifying and Reducing the Money Laundering Risks Posed by Individuals Who Have Been Unknowingly Recruited as Money Mules." *Journal of Money Laundering Control* 24, no. 1 (May 2021): 201–12. <https://doi.org/10.1108/JMLC-05-2020-0053>.
- Federal Bureau of Investigation. "2018 Internet Crime Report," April 22, 2019. <https://www.ic3.gov/Home/AnnualReports>.
- . "Don't Be a Mule." FBI News, December 17, 2018. <https://www.fbi.gov/news/stories/fbi-joins-international-campaign-to-stop-money-mules-121718>.
- . "FBI Warns of Money Mule Schemes Exploiting the Covid-19 Pandemic," April 6, 2020. <https://www.fbi.gov/news/pressrel/press-releases/fbi-warns-of-money-mule-schemes-exploiting-the-covid-19-pandemic>.
- . *Internet Crime Report 2021*. Washington, DC: Federal Bureau of Investigation, 2022. https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf.
- . "Money Mules." Scams and Safety. Accessed April 21, 2022. <https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/money-mules>.
- Financial Action Task Force. *Professional Money Laundering*. Paris: Financial Action Task Force (FATF), 2018. www.fatf-gafi.org/publications/methodandtrends/documents/professional-money-laundering.html.

- Financial Crimes Enforcement Network. “Advisory on Illicit Activity Involving Convertible Virtual Currency.” Financial Crimes Enforcement Network (FinCEN), May 9, 2019. <https://www.fincen.gov/resources/advisories/fincen-advisory-fin-2019-a003>.
- . *Updated Advisory on Email Compromise Fraud Schemes Targeting Vulnerable Business Processes*. Financial Crimes Enforcement Network (FinCEN), 2019. <https://www.fincen.gov/resources/advisories/fincen-advisory-fin-2019-a005>.
- Florencio, Dinei, and Cormac Herley. “Phishing and Money Mules.” In *2010 IEEE International Workshop on Information Forensics and Security*, 1–5. Seattle, WA: IEEE, 2010. <https://doi.org/10.1109/WIFS.2010.5711465>.
- Forgas, Joseph P., and Roy F. Baumeister. “Homo Credulus: On the Social Psychology of Gullibility.” In *The Social Psychology of Gullibility: Fake News, Conspiracy Theories and Irrational Beliefs*, edited by Joseph P. Forgas and Roy F. Baumeister, 1–18. New York, NY: Routledge, 2019.
- , eds. *The Social Psychology of Gullibility: Fake News, Conspiracy Theories and Irrational Beliefs*. New York, NY: Routledge, 2019.
- Free, Clinton, and Pamela R. Murphy. “The Ties That Bind: The Decision to Co-Offend in Fraud.” *Contemporary Accounting Research* 32, no. 1 (March 2015): 18–54. <https://doi.org/10.1111/1911-3846.12063>.
- Gehman, Joel, Vern L. Glaser, Kathleen M. Eisenhardt, Denny Gioia, Ann Langley, and Kevin G. Corley. “Finding Theory–Method Fit: A Comparison of Three Qualitative Approaches to Theory Building.” *Journal of Management Inquiry* 27, no. 3 (July 2018): 284–300. <https://doi.org/10.1177/1056492617706029>.
- Gillespie, Alisdair A. “The Electronic Spanish Prisoner: Romance Frauds on the Internet.” *The Journal of Criminal Law* 81, no. 3 (June 2017): 217–31. <https://doi.org/10.1177/0022018317702803>.
- Gioia, Denny. “A Systematic Methodology for Doing Qualitative Research.” *The Journal of Applied Behavioral Science* 57, no. 1 (March 2021): 20–29. <https://doi.org/10.1177/0021886320982715>.
- Glaser, Barney G., and Anselm L. Strauss. *The Discovery of Grounded Theory: Strategies for Qualitative Research*. 5th ed. New York: Aldine Publishing Company, 2010.
- He, Xinlei, Qingyuan Gong, Yang Chen, Yang Zhang, Xin Wang, and Xiaoming Fu. “DatingSec: Detecting Malicious Accounts in Dating Apps Using a Content-Based Attention Network.” *IEEE Transactions on Dependable and Secure Computing* 18, no. 5 (2021): 2193–2208. <https://doi.org/10.1109/TDSC.2021.3068307>.

- Hunsicker, Lukayn. “Everything Financial Institutions Need to Know about Synthetic Identity Fraud—Thomson Reuters Institute.” Thomson Reuters, December 1, 2020. <https://www.thomsonreuters.com/en-us/posts/investigation-fraud-and-risk/synthetic-identity-fraud/>.
- Interpol. “Cybercrime.” Interpol. Accessed October 25, 2021. <https://www.interpol.int/content/download/5267/file/Cybercrime.pdf>.
- Kopp, Christian, Robert Layton, Jim Sillitoe, and Iqbal Gondal. “The Role of Love Stories in Romance Scams: A Qualitative Analysis of Fraudulent Profiles.” *International Journal of Cyber Criminology* 9, no. 2 (June 22, 2016): 205–17. <https://doi.org/10.5281/ZENODO.56227>.
- Krueger, Joachim I., Claudia Vogrincic-Haselbacher, and Anthony M. Evans. “Towards a Credible Theory of Gullibility.” In *The Social Psychology of Gullibility: Fake News, Conspiracy Theories and Irrational Beliefs*, edited by Joseph P. Forgas and Roy F. Baumeister, 103–22. New York, NY: Routledge, 2019.
- Lempert, Lora Bex. “Asking Questions of the Data: Memo Writing in the Grounded Theory Tradition.” In *The Sage Handbook of Grounded Theory*, edited by Antony Bryant and Kathy Charmaz. Los Angeles: SAGE, 2007.
- Madinger, John. *Money Laundering: A Guide for Criminal Investigators*. 3rd ed. Boca Raton, FL: Taylor & Francis, 2012.
- Mathers, Chris. *Crime School: Money Laundering*. Buffalo, NY: Firefly Books, 2004.
- Maulidi, Ach. “When and Why (Honest) People Commit Fraudulent Behaviours?: Extending the Fraud Triangle as a Predictor of Fraudulent Behaviours.” *Journal of Financial Crime* 27, no. 2 (January 13, 2020): 541–59. <https://doi.org/10.1108/JFC-05-2019-0058>.
- McIntosh Fuller, Kenethia L. “Personality and Crime: An Examination of the Influence of the Five Factor Model on Offending and Co-Offending.” PhD diss., Indiana University of Pennsylvania, 2012.
- Miller, Madison. “To Boldly Go Where No Metaverse Has Gone Before: A Virtual Reality Check.” Master’s thesis forthcoming, Naval Postgraduate School, 2023.
- Modic, David, and Stephen E. G. Lea. “How Neurotic Are Scam Victims, Really? The Big Five and Internet Scams.” *SSRN Electronic Journal*, 2012. <https://doi.org/10.2139/ssrn.2448130>.
- Monaghan, Ryan M. “Cybercrime Response Capabilities and Capacity: An Evaluation of Local Law Enforcement’s Response to a Complex Problem.” Master’s thesis, Naval Postgraduate School, 2020. <https://www.hsdl.org/?view&did=850258>.

- Nicholls, Jack, Aditya Kuppa, and Nhien-An Le-Khac. "Financial Cybercrime: A Comprehensive Survey of Deep Learning Approaches to Tackle the Evolving Financial Crime Landscape." *IEEE Access* 9 (December 2021): 163965–86. <https://doi.org/10.1109/ACCESS.2021.3134076>.
- Pratt, Travis C., Kristy Holtfreter, and Michael D. Reisig. "Routine Online Activity and Internet Fraud Targeting: Extending the Generality of Routine Activity Theory." *Journal of Research in Crime and Delinquency* 47, no. 3 (August 2010): 267–96. <https://doi.org/10.1177/0022427810365903>.
- QSR International. "About NVivo." NVivo. Accessed December 22, 2022. <https://help-nv.qsrinternational.com/20/win/Content/about-nvivo/about-nvivo.htm>.
- Raza, Muhammad Subtain, Qi Zhan, and Sana Rubab. "Role of Money Mules in Money Laundering and Financial Crimes a Discussion Through Case Studies." *Journal of Financial Crime* 27, no. 3 (May 2020): 911–31. <https://doi.org/10.1108/JFC-02-2020-0028>.
- Rosner, Eric. "Cyber Federalism: Defining Cyber's Jurisdictional Boundaries." Master's thesis, Naval Postgraduate School, 2017. <https://www.hsdl.org/?view&did=808202>.
- Schwandt, Thomas A. *The SAGE Dictionary of Qualitative Inquiry*. 4th ed. Los Angeles: SAGE, 2015.
- Sembler, Joseph. "Cryptocurrency: Changing the Game for State and Local Law Enforcement." Master's thesis forthcoming, Naval Postgraduate School, 2023.
- Sorell, Tom, and Monica Whitty. "Online Romance Scams and Victimhood." *Security Journal* 32, no. 3 (September 2019): 342–61. <https://doi.org/10.1057/s41284-019-00166-w>.
- Sternberg, Robert J. "A Triangular Theory of Love." *Psychological Review* 93, no. 2 (April 1986): 119–35. <https://doi.org/10.1037/0033-295X.93.2.119>.
- Suarez-Tangil, Guillermo, Matthew Edwards, Claudia Peersman, Gianluca Stringhini, Awais Rashid, and Monica Whitty. "Automatically Dismantling Online Dating Fraud." *IEEE Transactions on Information Forensics and Security* 15 (2020): 1128–37. <https://doi.org/10.1109/TIFS.2019.2930479>.
- The Swartz Law Firm. "Hiding Cash Payments from the IRS for Luxury Car Purchases Resulted in Conviction." *Swartz Law Firm Civil & Criminal Trial Law* (blog), November 26, 2018. <https://www.whitecollarcriminaldefenselawyerblog.com/hiding-cash-payments-from-the-irs-for-luxury-car-purchases-resulted-in-conviction/>.

- United Nations. “Midterm Report of the Panel of Experts Submitted Pursuant to Resolution 2464 (2019).” United Nations, August 30, 2019. https://www.un.org/securitycouncil/sanctions/1718/panel_experts/reports.
- Unkelbach, Christian, and Alex Koch. “Gullible but Functional? Information Repetition and the Formation of Beliefs.” In *The Social Psychology of Gullibility: Fake News, Conspiracy Theories and Irrational Beliefs*, edited by Joseph P. Forgas and Roy F. Baumeister, 42–60. New York, NY: Routledge, 2019.
- Wang, Fangzhou, C. Jordan Howell, David Maimon, and Scott Jacques. *The Restrictive Deterrent Effect of Warning Messages Sent to Active Romance Fraudsters: An Experimental Approach*. Atlanta: CrimRxiv, 2020. <https://doi.org/10.21428/cb6ab371.c6eae022>.
- Whitty, M. T. “The Scammers Persuasive Techniques Model: Development of a Stage Model to Explain the Online Dating Romance Scam.” *British Journal of Criminology* 53, no. 4 (July 1, 2013): 665–84. <https://doi.org/10.1093/bjc/azt009>.
- Whitty, Monica. “Is There a Scam for Everyone? Psychologically Profiling Cyberscam Victims.” *European Journal on Criminal Policy and Research* 26, no. 3 (September 2020): 399–409. <https://doi.org/10.1007/s10610-020-09458-z>.
- Whitty, Monica T. “Anatomy of the Online Dating Romance Scam.” *Security Journal* 28, no. 4 (October 2015): 443–55. <https://doi.org/10.1057/sj.2012.57>.
- . “Do You Love Me? Psychological Characteristics of Romance Scam Victims.” *Cyberpsychology, Behavior, and Social Networking* 21, no. 2 (February 2018): 105–9. <https://doi.org/10.1089/cyber.2016.0729>.
- . “Predicting Susceptibility to Cyber-Fraud Victimhood.” *Journal of Financial Crime* 26, no. 1 (January 7, 2019): 277–92. <https://doi.org/10.1108/JFC-10-2017-0095>.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
Ft. Belvoir, Virginia
2. Dudley Knox Library
Naval Postgraduate School
Monterey, California



DUDLEY KNOX LIBRARY

NAVAL POSTGRADUATE SCHOOL

WWW.NPS.EDU

WHERE SCIENCE MEETS THE ART OF WARFARE