

# 基于扎根理论的贷款注销诈骗全过程心理交互机制

孙瑜滢, 沈欣

浙江工业大学教育学院, 浙江 杭州

收稿日期: 2026年4月23日; 录用日期: 2026年6月11日; 发布日期: 2026年6月29日

## 摘要

当前贷款注销诈骗危害突出, 作为典型避损型诈骗, 其心理操控机制尚缺乏系统研究。本研究基于141份受害者自述文本, 运用扎根理论和文本分析方法, 将诈骗过程分为接触与信任构建、控制与资金榨取、诈骗终止与创伤反应三个阶段, 梳理欺诈者行为、受骗者心理状态与行为演化规律。研究表明, 该类诈骗依托损失厌恶、权威伪装、信息隔离与心理施压实现欺诈, 受害者心理由初期怀疑警惕逐步走向认知瓦解, 受骗后产生自责、崩溃等负性情绪与心理创伤。本研究厘清了注销贷款诈骗完整演化链条, 可为反诈宣传防控与受害者心理干预提供理论参考。

## 关键词

贷款注销诈骗, 避损型诈骗, 扎根理论, 心理操纵

# The Whole-Process Psychological Interaction Mechanisms of Loan Cancellation Fraud Based on Grounded Theory

Yuxi Sun, Xin Shen

College of Education, Zhejiang University of Technology, Hangzhou Zhejiang

Received: April 23, 2026; accepted: June 11, 2026; published: June 29, 2026

## Abstract

Loan cancellation fraud has become increasingly prevalent and harmful at present. As a typical loss-

avoidance type of fraud, it still lacks systematic research on its psychological manipulation mechanism. Based on 141 victim self-narrative texts, this study adopts grounded theory and textual analysis to divide the fraud process into three stages: contact and trust establishment, behavioral control and financial exploitation, as well as fraud termination and traumatic reactions. It further summarizes the behavioral patterns of fraudsters and the psychological and behavioral evolution of victims. The results indicate that such fraud is realized through loss aversion, authority disguise, information isolation and psychological pressure. Victims gradually fall from initial suspicion and vigilance to cognitive collapse, and subsequently suffer from negative emotions such as self-blame and breakdown, accompanied by severe psychological trauma. This study clarifies the complete evolutionary chain of loan cancellation fraud, and provides theoretical references for anti-fraud publicity, targeted prevention and psychological intervention for victims.

## Keywords

Loan Cancellation Fraud, Loss-Avoidance Fraud, Grounded Theory, Psychological Manipulation

Copyright © 2026 by author(s) and Hans Publishers Inc.

This work is licensed under the Creative Commons Attribution International License (CC BY 4.0).

<http://creativecommons.org/licenses/by/4.0/>



Open Access

## 1. 引言

当前, 电信网络诈骗犯罪长期处于高位运行状态, 给受害者带来严重的身体伤害(Buttton et al., 2014)和心理创伤(Cross, 2015; Ganzini et al., 1990), 严重影响社会公众安全感和满意度。研究发现, 电信网络诈骗可分为刷单返利类诈骗、虚假网络投资理财类诈骗、虚假购物服务类诈骗、冒充电商物流客服类诈骗、虚假贷款类诈骗、冒充熟人类诈骗、注销贷款类诈骗、冒充公检法及政府机关类诈骗、网络婚恋和交友类诈骗、网络游戏产品虚假交易类诈骗等十种类型。其中, 注销贷款类诈骗作为电信诈骗的重要类型之一, 对人们的财务安全构成了严重的威胁。然而, 当前仍然缺少实证研究调查注销贷款类中诈骗者的手段、受害者的反应及心理状态。

贷款注销诈骗是指诈骗分子冒充银行工作人员、中国银保监会或在线贷款平台人员, 谎称受害者存在信用问题或旧账户未注销, 需删除不良信用记录或注销相关账户, 否则将严重影响个人信用。随后, 欺诈者以“清理信用”或“注销账户”为由, 诱使受害者通过正规借贷平台或金融 APP 申请贷款, 并将所贷资金转入诈骗分子控制的账户, 最终导致资金损失的欺诈行为(Wang et al., 2024)。此类诈骗往往借助高度仿真的钓鱼信息模仿权威机构(如银行或政府部门), 以提升欺骗性(Pietri et al., 2025), 并通过威胁法律后果制造恐惧、提出虚假问题的“解决方案”、营造紧急情境施加心理压力, 迫使受害者在未充分思考的情况下仓促行动(Liu et al., 2025)。因此, 贷款注销诈骗是一种剧本化、精细化的电信诈骗, 其核心特征在于欺诈者精准利用受害者对个人信用受损与法律责任的深度恐惧。

根据诈骗动机与手段的不同, 常见诈骗类型可分为“趋利型诈骗”与“避损型诈骗”(Lyu et al., 2025)。趋利型诈骗通过制造“获利”情境骗取受害者初始信任, 进而诱发其决策偏差; 而避损型诈骗则通过捏造“意外事件”、营造“损失”情境引发受害者不安全感, 同样导致非理性决策(Chen et al., 2023)。贷款注销诈骗属于典型的避损型诈骗, 其不承诺任何未来收益, 而是以征信污点、高额债务、法律诉讼等严重后果相威胁, 迫使受害者为避免损失而顺从操作。值得注意的是, 随着技术进步, 避损型诈骗的操纵手段日趋精密。生成式人工智能(AI)的广泛应用显著增强了社会工程攻击的逼真度与针对性, 进一步放大受害者的恐惧感与“损失厌恶”心理, 使此类诈骗的欺骗性达到前所未有的高度(Pietri et al., 2025)。

避损型诈骗通常借助紧迫感与恐惧心理实施操控。对真实诈骗通话录音的分析显示, 欺诈者常采用重复语句、强行打断、提高音量、放大嗓门等威胁性沟通技巧, 以引发受害者的心理恐慌(Chen, 2021)。从认知心理学角度看, 个体对损失的敏感度通常高于对等额收益的反应(Fung, 2015), 损失带来的心理痛苦远大于获取等额利益时的快乐(Tversky & Kahneman, 1991), 这种“损失厌恶”倾向使人在面对潜在损失时更容易做出非理性决策。在贷款注销诈骗中, 欺诈者正是利用这一认知偏差, 通过激发受害者对信用损失和法律责任的恐惧——而非对利益的贪婪——来诱导其顺从行为。

为强化心理压迫, 诈骗者频繁使用威胁性话术, 如“不及时注销将影响征信”“需支付手续费解除风险”等, 刻意引发受害者的负面情绪。这种策略导致受害者“情绪唤醒急剧升高”(Ignatova, 2024), 进而削弱其理性判断与信息处理能力(Cukier & Nesselroth, 2007; Workman, 2008)。与此同时, 避损型诈骗往往伴随对受害者的逐步隔离与控制。研究表明, 疲劳、饥饿、社交隔离、时间压力及特定背景音乐等因素均可降低个体的意识控制水平(Bulatov, 2015)。在贷款注销诈骗中, 欺诈者常要求受害者在“安静环境”中操作, 并通过呼叫转移等技术手段切断其与外界的联系, 逐步诱导其从低成本的初步顺从(如提供个人信息), 升级至进行大额资金转账(Ignatova, 2024), 形成完整的行为操控链条。

营造真实感与权威性是此类诈骗的另一关键策略。Fischer et al. (2013)指出, 使用“官方”通知、标志等元素能有效提升交互过程中的可信度。在实际案例中, 欺诈者通过口述虚假证件编号、展示其掌握的受害者精准个人信息等方式, 塑造无所不能的权威形象, 进而利用受害者“对权力、法律和法庭的恐惧”实施操纵(Ignatova, 2024)。

“认知窄化”也是受害者陷入诈骗的重要认知机制。Wang et al. (2012)发现, “限时”信息往往比非紧急信息更能引发快速反应。因此, 欺诈者常以“工作繁忙”“处理时限紧迫”为由反复催促, 使受害者在时间压力下只能接受欺诈者提供的单一叙事框架, 机械遵循指令(Ignatova, 2024), 丧失灵活思考与评估替代方案的能力。

从更广泛的视角看, 网络诈骗常利用人类信息处理模式的固有缺陷达成目的(Norris et al., 2019)。内在因素方面, 年龄较轻、教育程度较低、冲动性较高、信任倾向较强的个体更易受害; 外在因素方面, 经历负面生活事件、社会支持薄弱的群体风险更高(Zhang & Ye, 2022)。Xu 等人(2024)进一步指出, 认知成熟度、易受说服力与风险感知获益等心理因素在预测诈骗易感性方面可能比人口学变量更具解释力。

欺诈者善于利用多样化在线平台寻找并接触目标。研究表明, 诈骗实施高度依赖特定媒体类型(如 QQ、微信、支付宝等), 且不同诈骗类型与平台之间存在显著关联(Lee, 2021)。然而, 这类研究多停留在宏观的“模式识别”与“平台归类”层面, 虽揭示了 QQ 与退款诈骗等关联, 却未深入剖析欺诈交互中双方动态的心理过程与微观操纵机制。类似地, Cross (2018)从受害者与司法网络角度提出了反诈建议, Tun & Birks (2023)在犯罪脚本自动提取方面取得进展, 但其重点仍在于行为序列识别, 对操纵策略与受害者心理决策之间的深层互动尚未展开实证探讨。换言之, 现有研究揭示了诈骗“在何处”发生, 但对“如何”通过心理操控逐步达成诈骗目的的微观机制, 仍缺乏系统、深入的洞察。

因此, 本研究旨在通过分析网络诈骗受害者的叙事文本, 识别欺诈者在不同阶段采用的具体心理操纵策略, 描绘受害者在此过程中的心理状态变化轨迹, 并探索欺诈者策略与受害者反应之间的动态互动模式, 从而为网络诈骗的预防与干预提供基于心理过程的全新视角。

## 2. 研究方法

本研究旨在探究注销贷款类诈骗中诈骗者的手段以及受害者的反应与心理状态。研究聚焦于已遭受诈骗并产生实际经济损失的个体, 旨在系统识别导致其陷入骗局并造成财产损失的关键影响因素。研究采用基于词典的文本分析和扎根理论编码方法(分析框架见图 1), 对受害者撰写的自身遭遇诈骗的经历文

本进行分析。首先, 我们通过网络爬虫技术从知乎和豆瓣平台抓取遭遇诈骗经历的相关帖子, 经筛选后构建有效文本数据集。随后对筛选出来的每条帖子进行清洗处理, 保留描述受害者经历的文本内容, 并将其划分为接触、引导操作、发现受害三个阶段。最后对各阶段有效文本进行分析, 从而获取不同诈骗阶段诈骗者的手段、受害者的反应及心理状态。

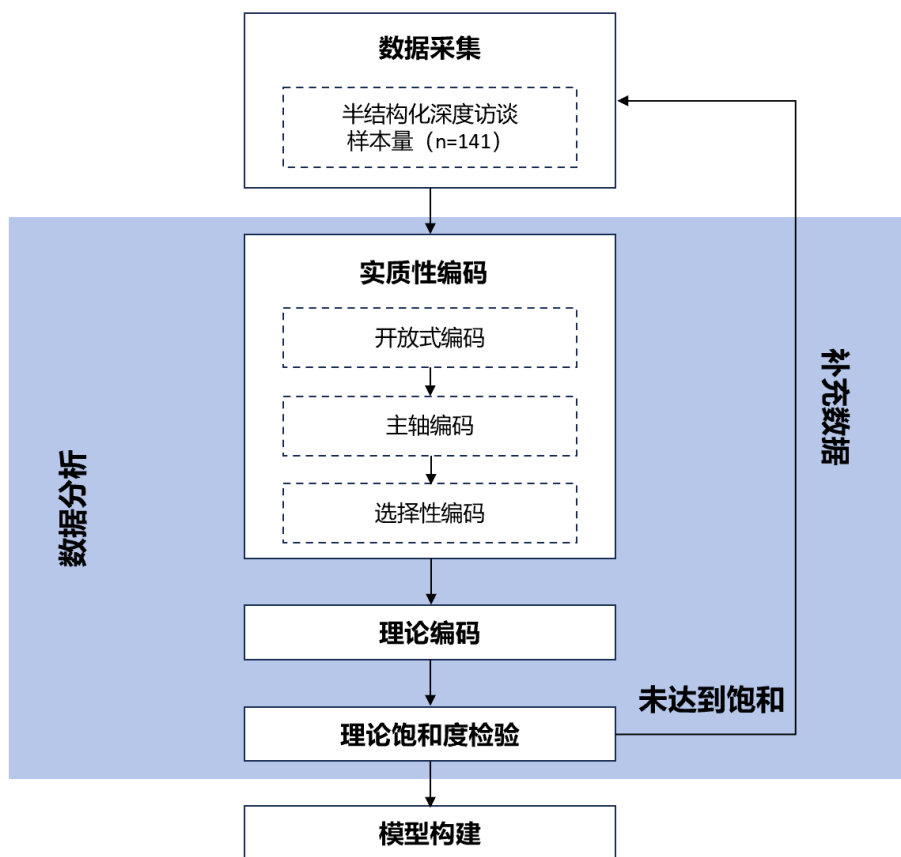


Figure 1. Analysis framework based on grounded theory  
图 1. 扎根理论分析框架

### 2.1. 数据收集

本研究对知乎和豆瓣平台上所有与诈骗受害相关的帖子进行了全面的爬取。上述平台作为国内颇具影响力的知识分享社区, 为用户提供了个性化的内容创作与表达空间(Cai & Shi, 2022)。用户在平台可选择使用化名登录与匿名发表, 帮助他们更完整、真实的披露受害经历(Clark-Gordon et al., 2019; Schlosser, 2020)。近年来, 随着网络诈骗的盛行, 越来越多受害者开始在平台上分享经历并警示潜在受害者。为此, 本研究收集了该社交平台上的受害者帖子, 随后对所有原始帖子进行筛选, 剔除重复发帖、非文本格式内容及与网络诈骗经历无关的帖子(例如反欺诈宣传广告、新闻报道、信息不完整的陈述、未产生实际经济损失的案例, 以及非受害者主动陈述的内容)。同时整合了同一用户发布的多条内容(即当用户发布多条帖子时, 我们将这些内容合并为一条记录)。最终数据集包含 141 条帖子, 对应 141 名用户。所有收集的帖子均为中文撰写, 后续分析也全程使用中文进行。

本研究为公开数据的回顾性分析。研究伦理委员会已确认无需伦理审批。所有数据收集与分析方法均按照相关指南和法规执行。

## 2.2. 数据分析

我们首先对 141 条有效帖子进行基础信息编码, 包括诈骗类型、损失金额和诈骗时间等信息, 以初步描绘网络诈骗受害的整体样貌。随后, 我们对每条帖子进行文本清洗, 排除了与诈骗者手段、受害者遭遇诈骗时的行为、想法和感受无关的内容。接着, 根据诈骗过程将清洗后的文本手动划分为不同阶段: 接触阶段(早期/阶段 1)、引导操作阶段(中期/阶段 2)和发现受害阶段(晚期/阶段 3)。接触阶段指受害人初次接触诈骗信息、产生兴趣并决定进一步参与的时期; 引导操作阶段指受害人被诱导深入互动、持续参与直至发觉受骗的过程; 发现受害阶段则聚焦于受害人察觉被骗之后的心理与反应。

在完成上述文本数据的预处理后, 我们使用 Nvivo 软件, 对每个案例的各阶段文本进行分析。我们对文本中所描述的诈骗互动过程进行逐级编码, 归纳出诈骗者行骗手法的完整脉络。最终共提炼出 26 种具有代表性的诈骗手段, 例如“假装客服”“引导参与刷单任务”等。同时, 为探究受害者在欺诈过程中的心理变化, 本研究对自述文本中受害者的心理状态进行了系统编码。通过对受害者诈骗不同阶段的叙述进行逐层分析, 最终识别并归纳出包括“怀疑”“愤怒暴躁”“焦虑”“懊悔”在内的 21 种具有代表性的心理状态。为系统分析受害者在欺诈过程中的行为模式, 我们对不同诈骗阶段中受害者的关键行为反应进行文本编码与归类, 最终提取出 16 种典型行为反应, 主要包括“向诈骗方转账”“通过借贷筹集资金”“向亲友求助”“延迟报案”等代表性行为。

为确保将文本划分为三个诈骗阶段的流程具备可靠的信度, 我们参照相关方法学建议(Potter & Levine-Donnerstein, 1999), 从所有案例中随机抽取 10% 的样本, 由两位研究者依据既定的编码手册, 独立完成文本阶段划分。经评估, 两位研究者划分结果的一致性较高, 平均 Kappa 系数为 0.86, 表明该文本划分步骤具有较好的信度。

## 3. 结果

本研究采用自下而上的扎根理论方法, 构建了贷款注销诈骗过程中欺诈者与受骗者互动的三阶段模型。在本节中, 我们将围绕欺诈者行为、受骗者心理状态、受骗者行为这三大核心因素展开(编码情况见表 1), 同时阐明这三大因素在接触与信任构建阶段、控制与资金榨取阶段、诈骗终止与创伤反应阶段的动态演变与交互影响。

**Table 1.** Coding categories

**表 1.** 编码类别

选择性编码	主轴编码	自由编码总频次
欺诈者操控策略	权威伪装	325 (14.88%)
	信息先占	104 (4.76%)
	问题制造	133 (6.09%)
	心理操控	189 (8.65%)
	行为隔离	38 (1.74%)
	技术监控	57 (2.61%)
	突然消失	43 (1.97%)
	继续诈骗	91 (4.17%)
受骗者心理状态	担忧	20 (0.92%)
	怀疑	83 (3.80%)

续表

	慌张	59 (2.70%)
	迷茫	62 (2.84%)
	认知瓦解	23 (1.05%)
	后悔	86 (3.94%)
	自责	83 (3.80%)
	崩溃	158 (7.23%)
	创伤反应	72 (3.30%)
	有限防御	5 (0.23%)
	高度顺从	344 (15.75%)
受骗者行为反应	报警	116 (5.31%)
	止损	42 (1.92%)
	情绪宣泄	24 (1.10%)
	总数	2184 (100.00%)

### 3.1. 阶段一：接触与信任构建

此阶段是诈骗的起始环节，核心目标是欺诈者通过策略性行为打破受骗者的心理防线，建立初步信任关系。

欺诈者行为包括权威伪装、信息先占、问题制造三个方面。权威伪装指欺诈者往往冒充金融机构、公检法等具有高可信度的角色，利用受骗者对权威的敬畏和信任降低其警惕性。信息先占指欺诈者通过非法渠道获取受骗者的个人信息，如姓名、身份证号、银行卡号等，在沟通过程中“透露”，营造正规机构的假象，增强可信度。问题制造指欺诈者通过虚构“账户涉嫌借取非法校园贷”“信息泄露”等紧急事件，制造受骗者的焦虑与恐慌，迫使受骗者进入被迫应对状态。

受骗者心理状态则包括担忧、怀疑和被唤起的风险意识。担忧指受骗者对欺诈者制造的“贷款”问题感到担忧和紧张，主要表现为担心个人征信受到影响，个人隐私被泄露，财产安全受到威胁等。怀疑指在与欺诈者的初步接触中，受骗者会对欺诈者提及的贷款事件的真实性和对方身份存在怀疑和不确定。被唤起的风险意识指在欺诈者的话术引导下，受骗者的风险意识被短暂激活，但这种意识往往指向“如何解决问题”，例如如何“注销贷款”，而非“质疑事件本身”。

受骗者行为则包括试探性接触、有限防御和初步配合。试探性接触指受骗者按照指示通过 QQ、短信、电话等方式与欺诈者进行初步沟通，试图核实信息、了解情况。有限防御指在诈骗行为初期，受骗者仍保持一定的警惕，不会轻易进行转账或借贷等与财产相关的操作，表现出有限的防御。初步配合指在欺诈者的引导下，受骗者可能会按照指示进行一些初步操作，如添加“工作人员”联系方式、共享屏幕、同意远程控制等，以“配合操作”。

### 3.2. 阶段二：控制与资金榨取

此阶段是诈骗的核心环节，欺诈者通过心理操纵等手段完全控制受骗者，诱使其进行贷款注销，转移资金。

欺诈者行为包括心理操控、行为隔离、技术监控三个方面。心理操控指欺诈者往往反复催促、施压，“今天得赶紧帮您处理完遗留问题了，我们客服在开会时都被批评了”“是最后的期限”“到底还处不

处理”等等, 强化受骗者的焦虑和恐惧, 使其认知能力下降, 判断力丧失。行为隔离指欺诈者还会利用“找一个安静的地方”“处理时不能中断”等理由, 切断受骗者与家人、朋友等外界的联系, 将其孤立在一个封闭的信息环境中, 确保欺诈行为的进行。技术监控指欺诈者以“保证用户权益”“记录处理过程”等为借口获取受骗者的信任, 通过屏幕共享、远程控制软件等技术手段, 直接监控受骗者的各种操作, 套取受骗者的隐私信息。

受骗者心理状态则包括慌张、迷茫和认知瓦解。慌张指在持续的压力下, 受骗者会感到极度恐慌, “资金套出来之后我非常紧张, 就想着要怎么赶紧转还回去”, 内心不安。迷茫指在欺诈者的操纵下, 受骗者往往思维混乱, “到此脑子全程懵了”“混沌在其中”, 失去了对当下信息的判断能力。认知瓦解指受骗者无法理性分析信息的真伪, 完全被欺诈者的话术所主导, “觉得套出来的不是我的钱”“就是想着赶紧清除这些借贷信息免得后续征信影响”, 陷入“为了自保必须照做”的认知误区。

受骗者行为则包括高度顺从执行, 如借贷、转账、借钱。受骗者会无条件地按照欺诈者的指示进行操作, 为了“保护征信”或“避免其他损失”, 从各个网贷平台借取网络贷款, 甚至向周围亲戚朋友借钱, 将钱款转入欺诈者指定的账户, 以对贷款进行“核销”。

### 3.3. 阶段三：诈骗终止与创伤反应

此阶段标志着诈骗行为的结束, 受骗者从被骗的噩梦中惊醒, 进入创伤后的心理与行为反应期。

欺诈者行为包括突然消失和继续诈骗两个方面。突然消失指在成功骗取钱款后, 欺诈者会立即切断与受骗者的所有联系方式, 让受骗者无法再与之联系, 彻底失联。继续诈骗指部分诈骗者会利用受骗者仍处于混乱中或希望挽回损失的心理, 实施二次诈骗。

受骗者心理状态则包括后悔、自责、崩溃和创伤反应。后悔指受骗者在意识到自己被骗后, 往往对自己的轻信和单纯感到极度后悔, “当时没想到”“应该先确认一下的”“当时要冷静一下的”等等。自责指受骗者会对遭受诈骗感到自责, 认为是自己的过错导致了财产损失, “我觉得自己是真的蠢”“怀疑自己”“自己太天真太好骗”等等。崩溃指在巨大的经济损失和精神打击下, 部分受骗者会出现情绪崩溃, “想哭但是哭不出来”, “只想一个人呆在房间里”“心态崩塌, 对不起所有人”等等。创伤反应指部分受骗者还会出现失眠、焦虑、抑郁等创伤后应激反应, “觉得度日如年”“常常一宿未睡”“痛苦未眠”等等, 严重影响其正常生活。

受骗者行为则包括报警、止损和情绪宣泄。报警指意识到被骗后, 绝大部分受骗者会第一时间向公安机关报案, “直接报警”“在警局做笔录”, 以寻求法律帮助。止损指在冷静下来分析欺诈已成事实后, 部分受骗者会尝试联系银行冻结账户、申请止付, 或向网贷平台说明情况, 阻止损失进一步扩大。情绪宣泄指受骗者会通过向家人、朋友倾诉, 或在网络社交平台分享被骗经历, “希望大家提高警惕”“才发现有类似经历的网友, 可以多聊聊”, 释放内心的压力和痛苦。

### 3.4. 模型总结

综上所述, 如图 2 所示, 在阶段一, 欺诈者通过权威伪装和问题制造, 引发受骗者的担忧与怀疑, 促使其进行下一步的试探性接触。在阶段二, 欺诈者通过心理操控和行为隔离, 瓦解受骗者的认知, 迫使其高度顺从并转移资金。在阶段三, 欺诈者的突然消失或继续诈骗, 触发了受骗者的后悔与崩溃, 促使其采取报警、止损等应对行为。

在整个诈骗过程中, 不同阶段欺诈者动态采取相应的行为, 直接塑造了受骗者的心理状态: 从怀疑到慌张地照做, 也导致了受骗者行为的转变: 从不配合到按照指示向特定账户转账, 驱动着贷款注销诈骗的实施。欺诈者行为、受骗者心理状态、受骗者行为的动态变化揭示了贷款注销诈骗的完整链条, 为

后续的诈骗干预提供了重要依据。

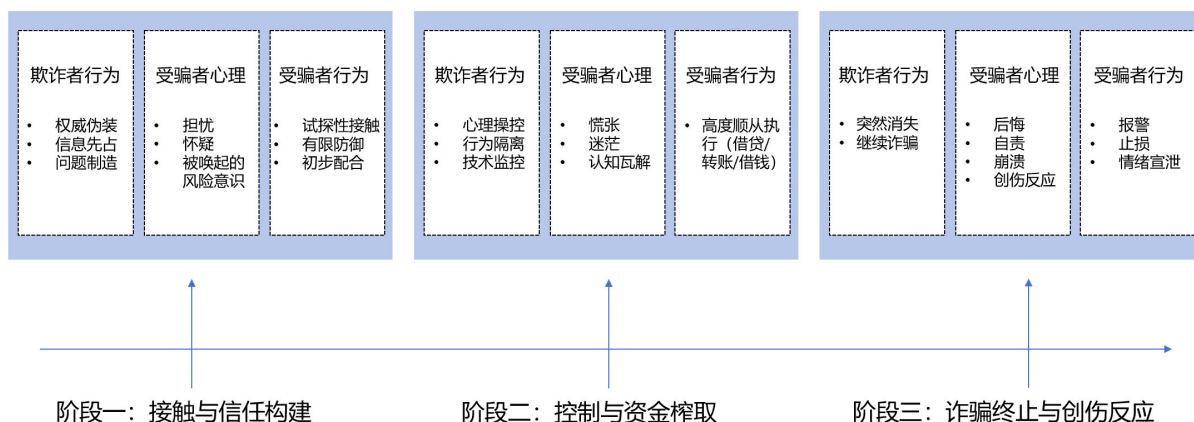


Figure 2. Grounded theory-based model

图 2. 基于扎根理论的模型

#### 4. 讨论

本研究以贷款注销诈骗为典型避损型电信网络诈骗，通过对 141 条受害者自述文本的扎根分析，构建接触与信任构建、控制与资金榨取、诈骗终止与创伤反应三阶段模型，揭示了欺诈者行为、受害者心理状态、受骗者行为的动态变化机制，弥补了该领域心理操纵机制实证研究的不足。

首先，本研究验证并拓展了避损型诈骗的核心心理机制。贷款注销诈骗不依赖利益诱惑，而是以征信受损、债务风险为威胁，激活受害者的损失厌恶倾向，从而导致非理性决策(Chen et al., 2023)。与趋利型诈骗相比，此类诈骗强化恐惧情绪和时间压力，引发受害者认知窄化，丧失了信息核验能力，仅聚焦于“避免损失”的单一目标，这与 Wang et al. (2012)提出的限时信息引发更强更快的反应高度契合。此外，与 Fischer et al. (2013)指出的一致，诈骗者往往利用“官方”通知展示权威性，且频繁使用威胁性话术使受害者“情绪唤醒急剧升高”(Chen, 2021)，进而组合行为隔离、技术监控等策略逐步诱导其从低成本的初步顺从(如提供信息复核)，升级至进行大额资金转账(Ignatova, 2024)。欺诈者的上述的操纵手段也与 Cialdini (1993)提出的说服力原则中的权威原则、承诺与一致原则高度一致。本研究呼应并揭示了这些原则在贷款注销诈骗情境下以“权威建立 - 恐慌制造 - 行为隔离 - 持续施压”的组合形式出现，构成了一个动态的操纵闭环。贷款注销诈骗结合心理操纵与技术手段，正朝着剧本化、精细化演变达到了前所未有的高度(Pietri et al., 2025)。

其次，本研究描绘了诈骗各阶段受害者全流程心理轨迹：从接触阶段的怀疑与警惕，到控制阶段的慌张、认知瓦解，再到意识到受骗后的后悔、自责、崩溃与创伤应激。这一连续变化表明，贷款注销诈骗对受害者的伤害不仅限于经济损失，更伴随着强烈负性情绪与心理创伤，这与已有研究指出的诈骗受害者易出现焦虑、抑郁等心理反应的结论一致(Cross, 2015; Ganzini et al., 1990)。此外，受害者在不同诈骗阶段的行为反应呈现被动升级特征，从试探接触、有限防御到高度执行借贷与转账操作，说明诈骗者的阶段性施压可逐步突破个体心理防线，而非单次诱导达成目的。

再者，本研究补充了现有文献对诈骗交互过程的认知缺口。既往研究多聚焦于诈骗类型、宏观风险因素、犯罪司法等(Zhang & Ye, 2022; Lee, 2021; Cross, 2018)，较少揭示诈骗者与受害者的动态互动逻辑。本研究发现，诈骗成功的关键并非单一固定话术，而是权威建立 - 恐慌制造 - 信息隔离 - 行为控制的闭环策略，这为理解网络诈骗提供了更细致的心理学解释。同时，受害者的风险意识在诈骗初期被错误引

导, 理性意识削弱(Cukier & Nesselroth, 2007; Workman, 2008), 仅关注“解决问题”而非“质疑事件”, 反映出公众在反诈认知上的结构性短板。这也深化了情境归因理论(Heider, 1944)在诈骗情境下的解释力, 欺诈者通过制造“征信受损”的外部情境压力, 将受害者的注意力转移到“解决外部问题”上, 从而使其产生将自身的顺从行为归因为“为了保护征信的理性选择”, 而非“被操纵的非理性行为”的归因偏差。

再次, 本研究为社会工程学模型提供了来自避损型诈骗的实证补充。传统社会工程学模型强调利用人性弱点获取信息, 本研究则发现, 在贷款注销诈骗中, 社会工程攻击已升级为包含心理、行为、技术的多维度操纵体系: 除了信息收集与权威伪装, 更包含了“损失厌恶”的情绪唤醒、行为隔离的环境控制等等。本研究的发现补充了社会工程学模型在避损型诈骗场景下的阶段特征, 揭示了其从“信息获取”到“资金榨取”的完整操纵链条。

最后, 本研究的发现具有实践启示。在反诈宣传中, 应针对性强化避损型诈骗心理操纵机制的科普, 提升公众对“权威来电”“危害征信”等典型套路的识别能力; 在技术防控方面, 反诈监管部门与相关平台应加强对远程控制、呼叫转移等诈骗工具的监测, 及时阻断诈骗者实施欺诈行为; 在诈骗结束期, 需为受害者提供心理支持服务, 缓解后悔、自责等负性情绪, 降低创伤后应激反应的持续影响。

同时, 本研究存在若干局限: 第一, 分析数据来源于网络自述文本, 可能存在回忆偏差, 主观性较高; 第二, 样本仅覆盖中文网络社交平台, 且未涉及不同年龄、地域、教育水平的群体差异; 第三, 研究未深入探究 AI 技术对诈骗手段的升级影响。

针对上述局限, 在此提出以下展望:

首先, 未来研究可重点整合三类核心数据源: 一是司法与金融类客观数据, 包括警方询问笔录、银行交易流水等, 通过与受害者自述文本对比, 校正主观回忆偏差, 还原诈骗交互的完整流程; 二是诈骗实施过程中的动态数据, 收集诈骗通话录音、屏幕共享录像、聊天记录等, 挖掘欺诈者语气节奏、话术逻辑的动态变化, 弥补静态文本分析的局限性; 三是第三方辅助数据, 引入反诈平台预警数据、征信机构相关数据、社区反诈宣传记录等, 为构建更全面的诈骗机制模型提供数据支撑。

其次, 为提升研究结论的普适性, 未来可重点从两个维度推进: 一是跨年龄段群体验证, 开展覆盖青少年、中青年、老年群体的大样本量化研究, 验证本研究构建的三阶段模型在不同年龄段人群中的适用性。二是跨文化模型验证, 选取征信体系、权威信任模式、互联网普及程度、文化价值观存在显著差异的国家和地区, 开展贷款注销类诈骗的比较研究, 对比不同文化背景下欺诈者的操纵策略、受害者的心理与行为反应差异, 探究文化因素对诈骗机制的影响。

最后, 随着 AI 技术的发展, 未来可结合 AI 技术特征, 开展跨学科分析, 探究技术升级背景下诈骗操纵机制的演变趋势。

## 5. 结论

从文化背景来看, 本研究样本来自中文网络社区, 文本数据来自知乎、豆瓣, 此类社交平台多以受教育程度较高、熟悉互联网操作的中青年为主, 且研究对象主要为中国境内的欺诈受害者。

本研究通过在特定文化背景下, 对特定网络社群的诈骗受害者的自述文本进行文本分析与扎根理论编码, 明确贷款注销诈骗的三阶段模型, 系统分析诈骗者的核心手段、受害者的心理变化与行为反应, 得出以下主要结论:

1) 贷款注销诈骗是典型的避损型诈骗, 核心逻辑是利用损失厌恶与权威恐惧, 通过心理施压与行为隔离实现资金榨取。

2) 诈骗过程呈现清晰的阶段递进特征: 接触阶段通过权威伪装与问题制造建立初步信任; 控制阶段以心理操控与行为隔离完成资金转移; 终止阶段诈骗者失联触发受害者创伤反应。

3) 受害者心理与行为随诈骗进程演变, 从初始防备警惕到高度顺从完成资金转移, 最终觉察陷入强烈负性情绪, 经济与心理双重受损。

4) 诈骗成功实施的关键在于利用认知窄化、信息隔离、威胁性沟通等多种心理操纵手段, 而非单一话术或技术手段。

综上所述, 本研究揭示了贷款注销诈骗的心理操纵机制与动态交互过程, 弥补了该领域实证研究的空白, 不仅为反诈宣传、技术防控及受害者支持工作提供了坚实的理论支撑, 也为后续相关研究搭建了可参考的分析框架、指明了具体的拓展方向, 同时为反诈防控提供了切实可行的实践指导。

## 基金项目

2025 年度大学生创新创业训练计划项目创业训练项目浙江省级一般项目推荐项目(S202510337133X)研究成果。

## 参考文献

- Bulatov, A. (2015). The Psychological Mechanisms of Fraud. *Legal Psychology, 16*, 215-222.
- Button, M., Lewis, C., & Tapley, J. (2014). Not a Victimless Crime: The Impact of Fraud on Individual Victims and Their Families. *Security Journal, 27*, 36-54. <https://doi.org/10.1057/sj.2012.11>
- Cai, Y., & Shi, W. (2022). The Influence of the Community Climate on Users' Knowledge-Sharing Intention: The Social Cognitive Theory Perspective. *Behaviour & Information Technology, 41*, 307-323. <https://doi.org/10.1080/0144929X.2020.1808704>
- Chen, H., Zhao, L., Guo, S., & Mo, L. (2023). How Do Telecom Frauds Lead to False Beliefs: Influencing Factors, Explanatory Theories, and Research Prospects. *Journal of South China Normal University (Social Science Edition), No. 2*, 94-106+207.
- Chen, J. (2021). "You Are in Trouble!": A Discursive Psychological Analysis of Threatening Language in Chinese Cellphone Fraud Interactions. *International Journal for the Semiotics of Law, 34*, 1065-1092. <https://doi.org/10.1007/s11196-020-09765-y>
- Cialdini, R. B. (1993). *The Psychology of Persuasion*.
- Clark-Gordon, C. V., Bowman, N. D., Goodboy, A. K., & Wright, A. (2019). Anonymity and Online Self-Disclosure: A Meta-Analysis. *Communication Reports, 32*, 98-111. <https://doi.org/10.1080/08934215.2019.1607516>
- Cross, C. (2015). No Laughing Matter: Blaming the Victim of Online Fraud. *International Review of Victimology, 21*, 187-204. <https://doi.org/10.1177/0269758015571471>
- Cross, C. (2018). Expectations vs Reality: Responding to Online Fraud across the Fraud Justice Network. *International Journal of Law, Crime and Justice, 55*, 1-12. <https://doi.org/10.1016/j.ijlci.2018.08.001>
- Cukier, W. L., Nesselroth, E. J., & Cody, S. (2007). Genre, Narrative and the "Nigerian Letter" in Electronic Mail. In *2007 40th Annual Hawaii International Conference on System Sciences (HICSS'07)* (pp. 70-70). IEEE. <https://doi.org/10.1109/hicss.2007.238>
- Fischer, P., Lea, S. E. G., & Evans, K. M. (2013). Why Do Individuals Respond to Fraudulent Scam Communications and Lose Money? The Psychological Determinants of Scam Compliance. *Journal of Applied Social Psychology, 43*, 2060-2072. <https://doi.org/10.1111/jasp.12158>
- Fung, M. K. (2015). Cumulative Prospect Theory and Managerial Incentives for Fraudulent Financial Reporting. *Contemporary Accounting Research, 32*, 55-75. <https://doi.org/10.1111/1911-3846.12074>
- Ganzini, L., McFarland, B. H., & Cutler, D. (1990). Prevalence of Mental Disorders after Catastrophic Financial Loss. *The Journal of Nervous and Mental Disease, 178*, 680-685. <https://doi.org/10.1097/00005053-199011000-00002>
- Heider, F. (1944). Social Perception and Phenomenal Causality. *Psychological Review, 51*, 358-374. <https://doi.org/10.1037/h0055425>
- Ignatova, E. S. (2024). Manipulation of Emotional Security by Cybercriminals Using Social Engineering Technologies: A Case Study. *Vestnik Permskogo universiteta. Filosofiiâ. Psihologiiâ. Sociologiiâ, 3*, 374-390. <https://doi.org/10.17072/2078-7898/2024-3-374-390>
- Lee, C. S. (2021). Online Fraud Victimization in China: A Case Study of Baidu Tieba. *Victims & Offenders, 16*, 343-362. <https://doi.org/10.1080/15564886.2020.1838372>
- Liu, X. F., Ai, Y., Jiang, L. C., Wang, X., & Wu, Y. (2025). Understanding the Human Element in Scams: A Multidisciplinary

- Approach. *Journal of Information Technology Case and Application Research*, 27, 9-24. <https://doi.org/10.1080/15228053.2024.2439192>
- Lwin Tun, Z., & Birks, D. (2023). Supporting Crime Script Analyses of Scams with Natural Language Processing. *Crime Science*, 12, Article No. 1. <https://doi.org/10.1186/s40163-022-00177-w>
- Lyu, C., Gao, S., & Zhang, Q. (2025). The Impact of Time Pressure and Type of Fraud on Susceptibility to Online Fraud. *Frontiers in Psychology*, 16, Article ID: 1508363. <https://doi.org/10.3389/fpsyg.2025.1508363>
- Norris, G., Brookes, A., & Dowell, D. (2019). The Psychology of Internet Fraud Victimization: A Systematic Review. *Journal of Police and Criminal Psychology*, 34, 231-245. <https://doi.org/10.1007/s11896-019-09334-5>
- Pietri, M., Mamei, M., & Colajanni, M. (2025). Telecom Spam and Scams in the 5G and Artificial Intelligence Era: Analyzing Economic Implications, Technical Challenges and Global Regulatory Efforts. *International Journal of Information Security*, 24, Article No. 139. <https://doi.org/10.1007/s10207-025-01062-8>
- Potter, W. J., & Levine-Donnerstein, D. (1999). Rethinking Validity and Reliability in Content Analysis. *Journal of Applied Communication Research*, 27, 258-284. <https://doi.org/10.1080/00909889909365539>
- Schlosser, A. E. (2020). Self-Disclosure versus Self-Presentation on Social Media. *Current Opinion in Psychology*, 31, 1-6. <https://doi.org/10.1016/j.copsyc.2019.06.025>
- Tversky, A., & Kahneman, D. (1991). Loss Aversion in Riskless Choice: A Reference-Dependent Model. *The Quarterly Journal of Economics*, 106, 1039-1061. <https://doi.org/10.2307/2937956>
- Wang, J., Herath, T., Chen, R., Vishwanath, A., & Rao, H. R. (2012). Research Article Phishing Susceptibility: An Investigation into the Processing of a Targeted Spear Phishing Email. *IEEE Transactions on Professional Communication*, 55, 345-362. <https://doi.org/10.1109/tpc.2012.2208392>
- Wang, J., Zhang, L., Xu, L., & Qian, X. (2024). The Dynamic Emotional Experience of Online Fraud Victims during the Process of Being Defrauded: A Text-Based Analysis. *Journal of Criminal Justice*, 94, Article ID: 102231. <https://doi.org/10.1016/j.jcrimjus.2024.102231>
- Workman, M. (2008). Wisecrackers: A Theory-Grounded Investigation of Phishing and Pretext Social Engineering Threats to Information Security. *Journal of the American Society for Information Science and Technology*, 59, 662-674. <https://doi.org/10.1002/asi.20779>
- Xu, L., Wen, X., Wang, J., Li, S., Shi, J., & Qian, X. (2024). Psychological Predictors of Online Fraud Victimization in China: A Machine Learning Approach. *Psychology, Crime & Law*, 32, 703-726. <https://doi.org/10.1080/1068316x.2024.2389187>
- Zhang, Z., & Ye, Z. (2022). The Role of Social-Psychological Factors of Victimhood on Victimization of Online Fraud in China. *Frontiers in Psychology*, 13, Article ID: 1030670. <https://doi.org/10.3389/fpsyg.2022.1030670>