Research Square

Preprints are preliminary reports that have not undergone peer review.
They should not be considered conclusive, used to inform clinical practice,
or referenced by the media as validated information.

Beyond Fraud Types: Guardian Severance and Relational Fraud Prevention in South Korea

Dongkyu Lee

shanner@kaist.ac.kr

Korea Advanced Institute of Science and Technology

Yongseok Seo

Korea Advanced Institute of Science and Technology

Research Article

Keywords: fraud prevention, relational fraud, guardian severance, ontology, crime script analysis, South Korea

Posted Date: November 10th, 2026

DOI: https://doi.org/10.21203/rs.3.rs-11178859/v1

License: This work is licensed under a Creative Commons Attribution 4.0 International License.
Read Full License

Additional Declarations: No competing interests reported.

Beyond Fraud Types: Guardian Severance and Relational Fraud Prevention in South Korea

Manuscript prepared for double-blind review — author-identifying information removed.

Abstract

Fraud prevention often responds to named scam types even when different scams rely on similar relational mechanisms. This study develops an ontology-informed relational framework for fraud prevention and applies it to five fraud types in South Korea. A structured cross-case analysis identifies a recurring five-stage relational core: trust construction, guardian severance, pressure creation, asset transfer, and concealment. Guardian severance—the offender's removal or circumvention of people, institutions, or systems that could interrupt the fraud—appears across all five cases, although its implementation varies. The analysis also shows that Korean reforms have strengthened information sharing and transfer-stage intervention without targeting guardian relationships. The study therefore proposes guardian restoration as a security-design principle and distinguishes ontological representation from both crime scripts and graph-based fraud detection.

Keywords: fraud prevention; relational fraud; guardian severance; ontology; crime script analysis; South Korea

1. Introduction

South Korea provides a useful setting for examining a persistent problem in fraud prevention: extensive investment in awareness, detection, and interagency coordination has not eliminated the capacity of fraud to adapt. Reported fraud offenses reached 421,421 in 2024, while voice-phishing losses were approximately KRW 854.5 billion (Financial Services Commission 2025; National Police Agency 2025a; Financial Supervisory Service 2025). Government responses have also become progressively more integrated. A one-stop 112 reporting and payment-suspension system was introduced in 2023, a national integrated

response structure was strengthened in 2025, and in 2026 new legal arrangements expanded cross-sector sharing of suspicious financial, telecommunications, and investigative information (Joint Government Ministries 2023; Joint Government TF 2026; Financial Services Commission 2026a). These reforms are consequential, but they also sharpen a theoretical question: what exactly should an integrated system represent and interrupt?

This article argues that one answer lies at the level of relational structure. Existing prevention commonly organizes fraud by named type—voice phishing, loan fraud, romance scam, team-mission fraud, secondhand-market fraud—or by the data domain of the institution that observes it. Such classifications are administratively useful, but they can obscure recurring relations among deceivers, victims, trust resources, guardians, pressure events, and transfer channels. The issue is not that contemporary fraud analytics are incapable of modeling relations. Graph-based methods increasingly represent accounts and transactions as nodes and edges and have improved the detection of networked financial fraud (Motie and Raahemi 2024). The narrower problem addressed here is semantic: relations represented for prediction are not necessarily typed in a way that preserves their security meaning across institutions and fraud forms.

The security problem is therefore not merely one of recognizing a growing catalogue of scam labels. Contemporary scams move across communication channels, platforms, financial institutions, and investigative jurisdictions, while offenders can substitute one delivery or payment mechanism for another. A prevention architecture organized only around observable surface features risks becoming method-dependent: the intervention remains effective against the feature it blocks, but the underlying manipulation can be reimplemented elsewhere. A relational approach instead asks which security functions must still be achieved for the fraud to succeed when the channel changes. This functional level of analysis connects

representation directly to the choice of intervention target and to the evaluation of security measures (Button et al. 2024; Johnson 2024).

To delimit the claim, the study concerns relational fraud: fraud in which offenders induce a victim to transfer assets by constructing, exploiting, or manipulating trust within the victim's decision environment. The category is defined by trust-mediated decision manipulation, not by the presence of guardian severance. It therefore excludes offenses such as unauthorized card use, pure account takeover, and internal accounting fraud that can succeed without inducing the victim's transfer decision. Whether protective relationships are weakened is treated as an analytical finding rather than a case-selection criterion.

The research question is: How can an ontological representation identify recurring relational operations across heterogeneous forms of relational fraud, and what security-prevention implications follow from that representation? The article makes three contributions. First, it specifies a fraud-focused ontology-informed relational schema that complements crime script analysis by formally distinguishing entities, roles, and relations that recur across fraud types. Second, through structured comparison of five Korean fraud types, it identifies a proposed Relational Core consisting of trust construction, guardian severance, pressure creation, asset transfer, and concealment. Third, it develops guardian restoration as a prevention principle: security measures should not only block the final transfer but also preserve or reconstruct the victim's access to independent verification and protective relationships before transfer occurs.

2. Relational Representation, Crime Scripts, and Ontology

2.1 From variable-centric to relational representation

Earlier fraud-detection systems frequently treated the transaction or account as the primary analytical unit and represented it through attribute vectors such as amount,

frequency, location, or account history (West and Bhattacharya 2016). This representation is effective for many detection tasks but can lose the structure that gives an otherwise ordinary transaction its meaning. The same transfer can be legitimate or fraudulent depending on who induced it, what authority or trust was invoked, whether verification channels were disabled, and how the transfer relates to preceding communications.

Recent graph learning reduces this limitation by modeling relationships directly. A systematic review by Motie and Raahemi (2024) shows that graph neural networks are now widely used to represent customers, accounts, merchants, and transactions as connected nodes and edges. Ontology-based knowledge integration has also been explored in financial fraud settings (Abrouk et al. 2024). This development matters for the present argument because it means that a contemporary critique cannot simply oppose "variable-centric" and "relational" analytics. The remaining gap is better described as one of semantic representation. A transaction edge in a financial graph may show that money moved between accounts, while an ontology can additionally represent that an actor impersonated an institution, exploited a trust resource, severed a guardian relationship, and induced a transfer within one persistent fraud event. Graph structure and ontology are therefore complementary rather than competing approaches.

Drawing on ontological realism, this article uses ontological poverty to denote a representational condition in which a schema omits distinctions and relations that are important to the target domain (Smith and Ceusters 2010; Arp, Smith, and Spear 2015). The term is used here as an analytical construct, not as a claim that existing systems contain no relational information. In fraud prevention, ontological poverty occurs when institution-specific records cannot express the same event and its security-relevant relations in a shared and persistent form.

Three distinctions are important. First, relational representation is not synonymous with ontology: a graph may represent many connections without assigning them domain-stable meanings. Second, semantic typing is not simply richer labeling. It allows two observations recorded by different institutions to be treated as instances of the same kind of relation while retaining provenance about where each observation originated. Third, persistence matters. A fraud event can pass from a telephone call to an application installation, a bank transfer, and a cash withdrawal; if each record is treated as a separate object, analysts may detect local anomalies without representing one continuing event. The proposed framework therefore treats ontology as a layer of shared meaning that can sit above heterogeneous operational systems rather than as a substitute for graph analytics, machine learning, or institutional databases.

2.2 Crime script analysis and the value of an ontological complement

Crime script analysis is particularly well suited to fraud because it decomposes offending into procedural stages and identifies points at which intervention is possible (Cornish 1994; Cornish and Clarke 2008; Haelterman 2016). Romance-scam research, for example, has shown how offenders construct relationships, isolate victims from alternative viewpoints, and escalate commitment over time (Whitty 2013; Choi, Jang, and Seo 2025). Script analysis also remains central to situational crime prevention because it connects offender decisions with practical opportunities for disruption.

The present framework extends rather than replaces that tradition. Crime scripts are intentionally crime-specific and sequence-oriented: they ask how a particular offense is accomplished. An ontology asks a different question: which kinds of entity and relation recur across different scripts, and can those relations be represented consistently when the surface method changes? Script analysis can describe a scene in which an offender tells a victim not

to contact family. Ontological representation can type that event as a change to a guardian–victim relation and compare it with technically different operations, such as malicious call interception or the removal of an escrow safeguard. The additional value is formal cross-typological comparability, not a claim that scripts are unable to discuss relationships. This emphasis on translating criminological insight into prevention practice is consistent with recent work on evidence-informed fraud prevention and prospective situational crime prevention (Button et al. 2024; Johnson 2024).

The concept of guardianship provides the criminological bridge between the two approaches. Routine activity theory usually asks whether a capable guardian is present in relation to a target (Felson 2008). Relational fraud adds a dynamic complication: the offender often acts directly on that protective relation. A family member can be made unavailable through secrecy instructions; a legitimate institution can be made unreachable through call interception; a platform safeguard can be bypassed by moving the transaction off-platform. The analytical object is therefore not only the presence of a guardian but the state of the victim–guardian relation over the course of the fraud. Modeling that relation explicitly makes it possible to compare different mechanisms according to the security function they disable.

Table 1. Crime script analysis and the ontological framework: complementary analytical roles

Dimension	**Crime script analysis**	**Ontological framework**
Primary question	How does this specific offense unfold?	What entities and relations recur across fraud types?
Representation	Procedural scenes and decisions	Typed entities, roles, and relations
Cross-type comparison	Possible through comparative scripting, but crime-specific by design	Direct through shared classes and predicates
Guardianship	Can be described as a scene or condition	Can be represented as a guardian–victim relation and its alteration
Prevention use	Disrupt scenes and opportunities	Identify recurring relational targets across scripts
Relationship to the other approach	Provides procedural granularity	Provides semantic comparability; intended as a complement

2.3 A three-layer prevention framework

The framework is ontology-informed rather than a formally implemented BFO/CCO ontology. It draws on ontological realism and on BFO and the Common Core Ontologies as examples of approaches that distinguish entities, roles, processes, and relations in a disciplined and interoperable way (Otte, Beverley, and Ruttenberg 2022; Beverley 2024). POL-INTEL is used only as an empirical illustration that object–relation representations can matter operationally in policing; Galis and Karlsson (2024) also show that such systems raise substantial questions of opacity, institutional power, and governance. The framework therefore does not treat a commercial platform as validation. It uses three analytical layers: a semantic layer specifying the entities and roles represented; a relational layer describing security-relevant operations among them; and an action layer linking those operations to possible preventive controls.

Consider a prosecutor-impersonation call as a simple illustration. At the semantic layer, the model identifies a deceiver, a victim, the invoked prosecutorial role as a trust asset, a legitimate verification channel as a guardian, and the receiving account as a transfer channel. At the relational layer, the deceiver exploits the trust asset, weakens or severs access to the guardian, increases pressure, and induces transfer. At the action layer, different controls can be attached to different relations: independent verification can protect the guardian link, transaction friction can affect the transfer relation, and number or account blocking can disrupt infrastructure. The layered representation is useful precisely because these controls need not be treated as alternatives; they act on different parts of the same event structure.

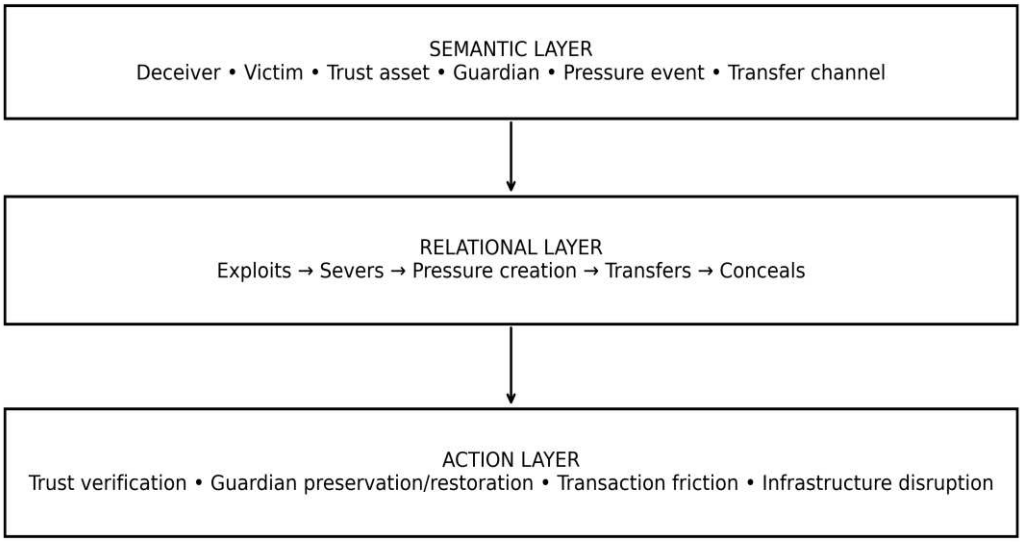


Figure 1. Ontology-informed relational prevention framework. The three layers separate what is represented, what relational operation is inferred, and what preventive action is considered. The framework is analytical, not a software architecture.

Figure 1 makes explicit how the layers are reused in the analysis: the five cases populate the semantic layer with different concrete actors and safeguards, the cross-case comparison asks whether they instantiate equivalent relational operations, and the security implications translate those operations into candidate controls. The same mapping is returned to in Sections 5 and 7.

3. Research Design and Methods

3.1 Design and case selection

The study uses a theory-building qualitative comparative design. Five Korean fraud types were selected through purposive maximum-variation sampling: composite institutional impersonation, direct prosecutor/regulator impersonation, low-interest loan refinancing fraud,

team-mission fraud, and secondhand-market non-delivery fraud. They differ in surface method, emotional leverage, transfer mechanism, and legal classification, making them useful for examining whether a common relational structure appears across heterogeneous cases. The selection is not statistically representative of fraud as a whole and is explicitly limited to relational fraud (Flyvbjerg 2006; Patton 2015).

Case inclusion followed three substantive criteria. First, the fraud had to depend on an induced decision by the victim to transfer money or another asset rather than on unauthorized appropriation alone. Second, the publicly documented method had to contain an identifiable process of trust construction, trust borrowing, or trust exploitation. Third, the five-case set had to provide maximum variation in surface method, emotional leverage, communication environment, and transfer mechanism. No case was selected because guardian severance was already known to be present. Protective relationships were coded only after case selection and script decomposition.

The five cases were not selected because they are the five most prevalent Korean frauds. They were chosen because they maximize variation in the means by which trust, pressure, protection, and transfer are organized. The two impersonation cases rely strongly on authority; loan refinancing fraud combines institutional trust with financial aspiration; team-mission fraud constructs a synthetic peer environment; and secondhand-market fraud relies on platform trust and the removal of transaction safeguards. Finding a common relation across such heterogeneous cases is more informative for theory building than repeatedly sampling closely related voice-phishing variants, while still falling short of population-level representativeness.

3.2 Sources and analytical procedure

Case descriptions were constructed from publicly available official statistics, government and police releases, statutes, and published reporting on representative incidents. Domain expertise within the author team informed recognition of typical method structures but was not treated as independent empirical evidence. No confidential case files or non-public police datasets were used. Documentary claims were cross-checked, where possible, against releases from the National Police Agency, Financial Services Commission, Financial Supervisory Service, or other responsible government bodies.

The documentary corpus was assembled around the selected fraud types rather than through a claim of exhaustive coverage of all Korean fraud reporting. Priority was given to official materials that described modus operandi, prevention advice, enforcement results, or institutional changes. Published academic work was used to establish criminological and fraud-process concepts. Where an operational detail could not be anchored to an official or published source, it was not treated as an evidential basis for the cross-case claim. This hierarchy is intended to separate the authors' interpretive expertise from the public evidence on which the analysis rests.

Analysis proceeded in two steps. First, each fraud type was decomposed into procedural scenes using crime-script logic. Second, those scenes were coded against the six classes and four relations in Table 2. Table 3 reports the cross-case stage mapping, while Supplementary Appendix A provides the source-to-code audit trail linking representative documentary evidence to each coded stage. Iterative comparison was then used to identify recurring operations across the five cases. The resulting Relational Core is a proposition derived from this bounded comparison and suitable for subsequent testing, not a universal law of fraud.

Coding was functional rather than lexical. For example, the phrases “do not tell your family”, malicious interception of outgoing calls, pressure to remain inside an offender-controlled group, and instructions to abandon a protected transaction channel use different words and technologies. They were coded together only when the observable effect was to reduce access to an independent source of protection or verification. Conversely, a stressful message was not coded as guardian severance merely because it created urgency; it was coded as a pressure event unless it also altered a protective relation. This distinction was used to avoid collapsing all persuasion into the focal construct.

The cross-case matrix was reviewed iteratively for both recurrence and disconfirmation. A candidate relation was retained in the proposed Relational Core only when an equivalent security function could be identified in all five selected cases. Ambiguous mappings were kept at the more conservative code. Supplementary Appendix A provides a source-to-code audit trail showing the representative documentary basis, observed mechanism, stage assignment, and ontological relation for each case. The appendix is intended to make the interpretive move from documentary description to relational abstraction transparent enough for replication or challenge.

3.3 Validity and limits

The design supports analytical rather than statistical generalization (Yin 2018). Maximum variation reduces the risk that the proposed core merely restates one fraud script, while public-source triangulation, an explicit codebook, and the supplementary source-to-code trail make the abstraction contestable. The principal limitation is interpretive: a small purposively selected case set can encourage post-hoc imposition of a preferred structure. A second limitation is geographical and institutional scope: all five cases are interpreted in the South Korean context, where platform practices, financial controls, reporting systems, and

legal categories shape what counts as an available guardian. The framework should therefore be tested in other jurisdictions as well as against additional relational frauds and deliberately selected negative cases. Quantitative validation with law-enforcement or financial-institution event data remains future work.

The strongest falsification test for the framework is therefore a negative case. If a relational fraud can reliably reach asset transfer while the victim retains effective independent verification and no protective relation is neutralized, the proposed centrality of guardian severance would be weakened. Similarly, the present study does not demonstrate that interventions aimed at guardian restoration are causally effective. It identifies a theoretically derived intervention target. Effectiveness requires prospective evaluation, ideally through field trials, quasi-experimental designs, or operational data that can compare victim outcomes when protective relationships are preserved versus when they are not.

4. The Representational Problem in Korean Fraud Prevention

Korean fraud prevention can be summarized through three mechanisms: public awareness, technology-based detection, and institutional intervention. Each is valuable, but each observes a different slice of the fraud process. Awareness campaigns are usually organized around recognizable scam types and therefore require continual updating as methods change. Detection is distributed across banks, telecommunications carriers, platforms, and law enforcement, each of which sees different data. Institutional interventions such as payment suspension, account controls, number blocking, and withdrawal delays operate most directly near the transfer or concealment stages.

The practical consequence is not simply “data silos.” It is that a single fraud event is represented differently across organizations. A spoofed call, malicious application, transfer to a mule account, and cash withdrawal can appear as separate objects in separate systems even

though they form one event. Ontological integration would require more than data exchange: it would require stable definitions of event identity, actor roles, protective relationships, and the relations connecting observations across domains. This distinction has become more important, not less, as graph and AI-based detection has improved within individual domains.

This distinction also clarifies what ontological integration would and would not achieve. It would not require every participating organization to use the same operational database or to disclose all customer-level information. Rather, institutions could retain local systems while agreeing on a limited set of shared semantic commitments: what counts as the same fraud event across records, which actor roles are relevant, how a protective relation is represented, and how evidence provenance is recorded. Such a design makes integration a governance problem as much as a technical one.

Korean policy has repeatedly shown the benefits and limits of transfer-stage intervention. A 2023 amendment extended victim relief to face-to-face collection scams after this method had grown from 3,244 cases in 2019 to 14,053 cases in 2022 (Financial Services Commission 2023). The episode illustrates substitution: when one transfer pathway becomes harder to exploit, offenders can change channels while preserving the broader deception process. This does not imply that account controls are ineffective; rather, it suggests that durable prevention benefits from identifying relational requirements that remain necessary when channels change.

Substitution should likewise be treated cautiously. The movement from account-based transfers toward face-to-face collection, cash couriers, virtual assets, or other channels does not prove that every intervention causes displacement. It does show that offenders have incentives to reroute activity around specific controls. For security design, the implication is to distinguish channel-dependent controls from relation-dependent controls. Blocking a mule account can be highly effective against that account; preserving an independent verification

relationship targets a condition that may remain relevant even when the payment route changes.

Recent reforms also reduce the force of any simple claim that Korea lacks integration. In June 2026, financial authorities introduced procedures allowing rapid temporary restrictions on accounts suspected of involvement in novel phishing and scam forms, including romance and no-show scams (Financial Services Commission 2026b). On 4 August 2026, amendments to the Telecommunications Financial Fraud Refund Act took effect and the ASAP information-sharing and analysis platform began operating with an expanded legal basis for pooling suspicious financial, telecommunications, and investigative information (Financial Services Commission 2026a). These are substantial advances. The question for this article is narrower: whether shared information is represented in a way that exposes recurring protective relationships as explicit intervention targets.

5. Cross-Case Findings: A Relational Core of Fraud

5.1 Ontological classes and relations

The comparative analysis uses six classes: deceiver, victim, trust asset, guardian, pressure event, and transfer channel. A trust asset is any resource used to construct apparent legitimacy, such as prosecutorial authority, a financial brand, a platform's reputation, or apparently successful group participants. A guardian is any person, institution, technical safeguard, or verification channel capable of interrupting the fraud. Four relations carry most of the analytical weight: exploits, severs, transfers, and conceals. Pressure creation is represented differently: Pressure Event is a class rather than a fifth predicate because the analysis treats urgency, threat, guilt, and sunk-cost escalation as event instances that can be generated through several different actor–victim relations. Table 2 defines this deliberately lightweight, ontology-informed schema rather than claiming a complete formal ontology.

Guardian is deliberately broader than a family member. Routine activity theory treats guardianship as the presence of a capable protector (Felson 2008), but in contemporary fraud the protective function may be supplied by a person, an institution, an escrow mechanism, an independent communication channel, or a platform control. Guardian severance therefore refers to the offender's removal, circumvention, or neutralization of a protective relation—not necessarily literal social isolation.

Table 2. Core ontological classes and relations

Element	Definition	Illustrative instantiations
Deceiver	Actor who misrepresents identity, authority, or intent	Fake official, loan officer, group operator, seller
Victim	Actor whose asset-transfer decision is manipulated	Call recipient, borrower, participant, buyer
Trust asset	Resource used to construct apparent legitimacy	Public authority, lender brand, platform reputation, shill success
Guardian	Person, institution, system, or verification channel able to interrupt the fraud	Family/adviser, legitimate agency, escrow, independent channel
Pressure event	Action that accelerates decision or suppresses reconsideration	Urgency, secrecy, guilt, sunk-cost escalation, scarcity
Transfer channel	Medium through which assets move	Bank transfer, cash courier, fake site, fake mall
Exploits (relation)	Deceiver → trust asset	Uses authority, brand, platform, or social proof
Severs (relation)	Deceiver → guardian–victim relation	Interception, secrecy, off-platform movement, synthetic group
Transfers (relation)	Victim → transfer channel	Executes material loss
Conceals (relation)	Deceiver → evidential/transfer infrastructure	Mule accounts, burner identities, deletion

5.2 The five-stage relational core

Across the five cases, comparison produced a recurring sequence: (1) trust construction, (2) guardian severance, (3) pressure creation, (4) asset transfer, and (5) concealment. Table 3 shows the cross-case mapping, and Supplementary Appendix A identifies representative documentary anchors for each stage. The sequence is functional rather than strictly chronological: stages may overlap, repeat, or be implemented through several channels. The analytical question is whether different scripts perform equivalent security functions, not whether every incident follows an identical timeline.

Case 1, composite institutional impersonation, provides the clearest technical form of guardian severance. Public warnings describe scams that begin with official-looking notifications or government impersonation, then direct the target toward malicious applications or controlled communication channels. The trust mechanism is borrowed institutional authority; the relevant guardian is independent contact with the genuine institution. Once an installed application can redirect calls or otherwise interfere with verification, the offender has changed the victim's relational environment rather than merely added another persuasive message. Pressure is then escalated through claims of investigation or asset protection, followed by transfer instructions. This case is coded as guardian severance because an independent verification path is made functionally unavailable, not simply because the victim is frightened (Financial Services Commission 2026c; Korea Internet & Security Agency 2026).

Case 2, direct prosecutor or regulator impersonation, reaches the same relational outcome without malicious software. Police descriptions of government-impersonation voice phishing show offenders using specific official roles, legal vocabulary, claims of criminal implication, and instructions that move the target away from third-party interference. The trust asset is asserted state authority; the guardian is access to family, advisers, or the real agency through an independently obtained number. When secrecy or investigatory-confidentiality claims suppress that consultation, the coded operation is guardian severance. Urgency and fear are coded separately as pressure events, and the later instruction to send money to a purported protective or verification account is coded as transfer (National Police Agency 2018).

Case 3, low-interest loan refinancing fraud, relies on financial aspiration rather than criminal accusation. Police and financial-authority materials describe approaches in which a supposed lender offers favorable refinancing but then requires repayment of existing debt, a

deposit, a guarantee, or installation of an application as a precondition. The trust asset is the apparent lender or policy-linked product. The protective relation may be a genuine bank channel, call-screening application, or independent comparison with the lender's official terms. Where the offender instructs the victim to delete protective applications, install malicious software, or remain within a controlled communication path, the protective relation is weakened before payment. The "repay first" demand and subsequent sunk-cost escalation are treated as pressure events rather than as severance itself (National Police Agency 2018; Financial Services Commission 2026c).

Case 4, team-mission fraud, provides a social-environmental form of the same operation. Police materials describe team-mission scams as a contemporary scam category involving repeated transfers through fraudulent task or investment applications, while response measures include analysis and blocking of scam-app infrastructure (National Police Agency 2026b). The analytical interest is the synthetic decision environment: apparent co-participants and the operator become the victim's immediate reference group, while repeated deposits and loss-recovery promises increase commitment. Guardian severance is coded only where the offender-controlled setting substitutes for independent verification or discourages exit; group pressure by itself is coded as a pressure event. This distinction prevents the framework from treating all social influence as severance.

Case 5, secondhand-market non-delivery fraud, is the most demanding boundary case and is therefore kept deliberately narrow. Police prevention material documents non-face-to-face "door-handle" trading in which buyers transfer funds before obtaining the item, sometimes followed by repeated payment demands and seller disappearance; the same material recommends direct face-to-face exchange and use of safe-transaction services (National Police Agency 2025b). A direct transfer is not automatically guardian severance. The severance code applies only when an offender actively induces the buyer to bypass or

abandon an available protected transaction mechanism or independent verification step. In that circumstance, an institutional safeguard is removed from the transaction before the irreversible transfer. This case therefore tests the outer boundary of the construct rather than serving as its easiest example.

Taken together, the five cases suggest three modes of guardian severance: technical severance, where malware or communication control impairs independent contact; authority-based or psychological severance, where secrecy or asserted obligation suppresses consultation; and environmental severance, where an offender-controlled group or transaction setting substitutes for an independent protective setting. The finding remains provisional. Guardian severance appeared in all five selected cases, but the analysis cannot establish that it is necessary for every relational fraud. Evidence that overseas organizations can operate several scam types at once is consistent with reusable underlying functions, but is treated here as corroborative rather than confirmatory evidence (National Police Agency 2026a).

Table 3. Cross-case mapping of the proposed Relational Core

Stage	Composite impersonation	Direct impersonation	Loan refinancing	Team-mission	Secondhand market
1 Trust construction	Fake payment + relay of officials	Prosecutor/FSS authority	Low-interest refinancing offer	Small payouts + shill success	Bargain listing + platform trust
2 Guardian severance	Malware/call interception	“Confidentiality” blocks consultation	Controlled app/channel; reduced verification	Offender-controlled group replaces independent reference points	Escrow refusal/off-platform payment
3 Pressure creation	Escalating fear	Victim-or-suspect urgency	Repay-first / sunk cost	Team-loss guilt + escalation	Scarcity/time pressure
4 Asset transfer	Fake site / account transfer	“Safe account” transfer	Transfer or cash courier	Repeated deposits	Direct transfer
5 Concealment	Mule accounts/burner infrastructure	Mule accounts/burner infrastructure	Mule accounts/couriers	Account deletion / mule infrastructure	Mule account/disappearance

5.3 What ontology adds to graph detection and scripts

The cross-case result clarifies both the contribution and the role of the three analytical layers. At the semantic layer, the same categories—victim, guardian, trust asset, transfer channel—can be instantiated by very different concrete entities. At the relational layer, call

interception, secrecy instructions, synthetic peer groups, and induced departure from a protected payment channel can be compared as candidate instances of one operation only when the codebook's criteria are satisfied. At the action layer, that shared representation supports a different question: which control would preserve or restore the protective relation before transfer? Graph-based fraud detection already captures network topology, and crime scripts already capture process and offender decision-making. Ontological representation adds explicit semantic typing across those different representations rather than replacing either of them (Motie and Raahemi 2024).

This difference can be expressed as a question of equivalence. Feature-based and graph-based models may distinguish several events because their observed attributes and edges differ. Ontological analysis asks whether those events instantiate the same higher-order relation for prevention purposes. The answer is not predetermined by the ontology; it depends on explicit definitions and evidence. That constraint is important because semantic abstraction can become too permissive if every unpleasant influence is labeled "severance". The codebook therefore requires an observable reduction, bypass, or substitution of an independent protective relation. This makes the construct potentially testable in operational data rather than merely metaphorical.

6. Institutional Transition and the Remaining Gap

Korea's response between 2023 and 2026 can be read as a transition from fragmented, type-specific action toward broader structural integration. The 2023 one-stop 112 system unified reporting and payment-suspension access. Measures introduced in 2025 strengthened integrated response and rapid blocking of criminal communication instruments. In 2026, authorities broadened temporary account restrictions for novel scams and created a legal basis for cross-sector suspicious-information sharing through the ASAP platform (Joint

Government Ministries 2023; Joint Government TF 2026; Financial Services Commission 2026a, 2026b).

These developments matter for the argument in two ways. First, they show that the policy system is already moving beyond narrow typologies. Second, they demonstrate why the distinction between data integration and semantic integration is now practically relevant. ASAP can concentrate and distribute suspicious information, but the public documentation reviewed for this study describes shared categories of financial, telecommunications, and investigative information rather than a shared ontology of fraud events and protective relations. Data sharing is a prerequisite for relational analysis, but it does not by itself determine how a guardian relation, trust asset, or cross-domain event identity is represented.

The transition can therefore be described as a move from organizational integration toward the possibility of semantic integration. Organizational integration creates channels through which agencies can cooperate; data integration permits records to be exchanged or jointly analyzed; semantic integration determines whether those records can be interpreted as parts of the same event with comparable roles and relations. The three are cumulative rather than interchangeable. Korea's recent reforms have materially advanced the first two. The present framework concerns the third.

Table 4 can be read through the same layers. The 2023 one-stop system primarily strengthened action-layer coordination by accelerating reporting and payment suspension. The 2026 suspicious-account measures extended intervention to a wider range of transfer patterns. ASAP is more consequential for the semantic and relational layers because it creates a legal and organizational environment in which records from telecommunications, finance, and investigation can be analyzed together. Public documentation, however, does not show that those records are yet governed by a shared vocabulary for guardian relationships, trust assets, or event identity. The remaining gap is therefore not a claim that Korea lacks

integration; it is a narrower claim about the representational terms on which integration operates.

Government reporting also showed seven consecutive months of declines in voice-phishing incidents and losses by May 2026 following intensified integrated measures (Joint Government TF 2026). This article does not attribute those declines causally to any single reform. The more limited observation is that publicly documented interventions remain concentrated on suspicious accounts, transfer channels, communication instruments, and post-report analysis. None of the reforms reviewed here explicitly institutionalizes guardian restoration as a general prevention objective. That remaining gap motivates the security-design implications below.

This is not an argument for redirecting resources away from transfer-stage controls. Payment suspension, number blocking, suspicious-account restrictions, and proceeds recovery can prevent or reduce harm even when earlier manipulation has succeeded. A layered prevention strategy would retain those controls while adding interventions earlier in the sequence. In security terms, guardian restoration is therefore a complementary upstream control rather than a replacement for existing downstream disruption.

Table 4. Korean institutional transition and the relational framework (2023–2026)

Change	Main effect	Relation to framework
One-stop 112 system (2023)	Unified reporting and payment-suspension access	Improves action-layer coordination
Integrated response expansion (2025)	Broader interagency operational coordination and blocking	Strengthens cross-domain analysis and action
Novel-scam suspicious-account restrictions (June 2026)	Rapid temporary restriction beyond classic voice-phishing patterns	Extends transfer-stage intervention across types
ASAP information-sharing framework (Aug. 2026)	Legal basis for pooling suspicious financial, telecom, and investigative information	Creates infrastructure for cross-domain representation
Remaining issue	Publicly documented reforms do not explicitly target guardian relationships	Potential semantic and prevention-design extension

7. Security Practice Implications

7.1 Guardian restoration as a design principle

The principal practical implication is to shift from a single proposed "universal intervention" to a more defensible design principle: when a fraud method depends on weakening independent verification, security systems should preserve or restore a guardian before irreversible transfer. The implementation should vary by context. For secondhand markets, platform-mediated escrow or friction against off-platform payment can preserve an institutional guardian. For high-risk transfers to new payees, an account holder could pre-designate a trusted contact or independent verification channel. For impersonation scams, banks and public agencies can design verification paths that cannot be reached through the same communication channel controlled by the caller.

Guardian restoration can be operationalized through three families of controls. Preservation controls keep an existing protection in place, such as preventing a high-risk marketplace transaction from being moved outside a protected payment environment. Reconnection controls restore an independent channel after an offender has narrowed the victim's information environment, for example by presenting a bank-generated verification route that cannot be reached through the caller-controlled device session. Diversification controls reduce dependence on any single communication channel by enabling a preselected second source of confirmation. The common design question is whether the proposed control changes the victim's access to independent verification before the irreversible transfer point.

Mapped to Figure 1, guardian restoration is an action-layer response to an observed relational-layer change rather than a new semantic class. This distinction matters because the same guardian concept can support different controls depending on whether severance is technical, psychological, or environmental.

This formulation also addresses privacy and autonomy concerns. Automatic disclosure of an adult's financial activity to family members would be inappropriate as a default and could create risks in coercive or abusive relationships. A trusted-contact mechanism should therefore be voluntary, revocable, and user-configurable. The general principle is not "notify family"; it is "introduce an independent verification relationship chosen or institutionally protected before high-risk transfer."

7.2 Relational warning signals and minimal-data detection

A second implication concerns detection. Systems can look for combinations that indicate protective relationships are being narrowed: transfer instructions coupled with claims of investigative secrecy, requests to leave an escrow environment, repeated instructions to avoid other information sources, or escalating group commitments controlled by one organizer. These signals should be treated as warning conditions rather than deterministic indicators of fraud. Their operational value would need to be tested against false positives and legitimate contexts.

Operational deployment would require calibrated thresholds and escalation rules. A single secrecy instruction or off-platform request may be legitimate; the security value lies in combinations, timing, and context. One possible architecture is staged escalation: a weak relational signal triggers only a warning or verification prompt, while a stronger combination of newly established payee, unusual transfer value, restricted verification, and known scam infrastructure triggers human review or temporary friction. Such a system should be evaluated on both fraud losses prevented and burdens imposed on legitimate users.

Relational detection may also support data minimization. A system need not construct a comprehensive behavioral profile of every customer if it can identify a narrow set of event-level relations relevant to imminent fraud. Ontology does not automatically solve privacy

problems—shared semantic infrastructure can enable surveillance as well as prevention—but it can make the data purpose explicit and auditable. A security architecture should therefore specify which relation is being detected, what evidence supports it, what action follows, and how long the underlying data are retained.

Governance should therefore be built into the representation. Each inferred relation should retain the source of the observation, confidence or evidential status, permitted purpose, retention period, and the action for which it may be used. This is especially important when data cross organizational boundaries. An ontology that standardizes meaning without preserving provenance could increase rather than reduce accountability problems. The proposed approach consequently treats semantic interoperability and evidential provenance as joint requirements.

7.3 From shared data to shared meaning

The institutional implication is not to replace current Korean reforms but to extend them. The 2026 information-sharing framework creates a stronger foundation for cross-sector detection (Financial Services Commission 2026a). The next step is semantic governance: agreeing on stable definitions for event identity, actor roles, transfer channels, protective relationships, and evidential provenance across participating organizations. Open standards such as BFO and the Common Core Ontologies offer one possible foundation, but the central requirement is institutional agreement, not adoption of a particular software product. Any shared vocabulary should remain intelligible to operational practitioners and should be evaluated by the quality of decisions it enables rather than by technical complexity alone.

A minimal shared fraud vocabulary need not begin with a comprehensive national ontology. A more feasible path would define a small number of high-value cross-sector objects and relations—event identity, actor role, claimed institution, transfer channel, protective relation,

and evidential source—then test whether these improve case linkage and prevention decisions. The vocabulary could expand only when an additional distinction produces operational value. This incremental approach favors operationally intelligible security practice and avoids turning an applied prevention proposal into a large technical standardization project.

7.4 An implementation and research agenda

The framework suggests a staged research program. First, retrospective validation should code a larger set of relational-fraud cases, including romance scams, investment-coaching scams, impersonation variants, and deliberately selected negative cases. Inter-coder agreement can then test whether guardian severance is identifiable without relying on the originating analyst. Second, operational studies should translate the construct into observable indicators and examine precision, false positives, and lead time before transfer. Third, intervention studies should test whether preserving or restoring independent verification changes victim behavior and loss outcomes.

Implementation should proceed with the same caution. A pilot could begin within one bounded domain—such as high-risk transfers to new payees or platform-mediated secondhand transactions—where the relevant guardian relationship is clearly defined. The pilot should specify the intended security function, the minimum data required, the user-facing intervention, override procedures, and review criteria before deployment. Success would not be measured only by detection accuracy. It would also require evidence that the intervention creates meaningful opportunity for independent verification without generating disproportionate friction, exclusion, or privacy intrusion.

8. Conclusion

This study reframes a portion of the fraud-prevention problem from the classification of scam types to the representation of security-relevant relations. Across five heterogeneous forms of relational fraud in South Korea, a proposed Relational Core was identified: trust construction, guardian severance, pressure creation, asset transfer, and concealment. The most useful finding is not that one sequence governs all fraud, but that technically different scams can perform the same security function—removing or bypassing independent protection before a victim transfers assets.

The shift is analytically important because scam labels describe what a fraud looks like, whereas security relations describe what the offender must accomplish within the victim's decision environment. That distinction permits prevention to remain sensitive to new surface methods without assuming that every new method requires an entirely new conceptual model.

The framework complements two established approaches. Crime scripts explain how a particular fraud unfolds, while graph-based analytics model network structure among transactions and actors. Ontological representation contributes explicit semantic typing across scripts and institutional data domains. This makes it possible to compare call interception, confidentiality pressure, synthetic peer groups, and escrow refusal as different implementations of guardian severance rather than unrelated scam features.

Korea's 2023–2026 reforms have significantly strengthened integrated reporting, suspicious-account intervention, and cross-sector information sharing. Those reforms make the proposed framework more, rather than less, relevant because data integration creates the conditions under which shared meaning matters. Future research should test the Relational Core against a wider range of relational fraud, seek negative cases, operationalize guardian-

severance indicators, and evaluate whether guardian-restoration interventions reduce victimization without disproportionate privacy costs.

Manuscript date: 27 September 2026. Word count: 6,174 words (abstract through conclusion; excluding tables, figure caption, and references).

References

Abrouk, Lylia, Hamza Chergui, Hamid Ahaggach, and Nicolas Cabioch. 2024. Enhancing fraud detection in SWIFT financial systems through ontology-based knowledge integration and graph-driven analysis. In Social network analysis and mining applications in healthcare and anomaly detection, ed. Mehmet Kaya, Sleiman Alhajj, Kashfia Sailunaz, and Min-Yuh Day, 267–289. Cham: Springer. https://doi.org/10.1007/978-3-031-75204-9_11.

Arp, Robert, Barry Smith, and Andrew D. Spear. 2015. Building ontologies with Basic Formal Ontology. Cambridge, MA: MIT Press.

Beverley, John. 2024. Common Core Ontologies (Version 2.0) [Software]. GitHub. https://github.com/CommonCoreOntology/CommonCoreOntologies.

Button, Mark, Branislav Hock, David Shepherd, and Paul Michael Gilmour. 2024. What really works in preventing fraud against organisations and do decision-makers really need to know? Security Journal 37: 965–983. https://doi.org/10.1057/s41284-023-00402-4.

Choi, H., S. Jang, and J. Seo. 2025. Romaenseu seukaem gwajeong-ui simnijeok yoin bunseok: Beomjoe seukeuripteu bunseok-eul jungsim-euro [An analysis of psychological factors in the romance scam process: A crime script analysis]. Gyeongchalhak Yeongu [Police Science Studies] 25 (2): 185–214.

Cornish, Derek B. 1994. The procedural analysis of offending and its relevance for situational prevention. In Crime prevention studies, vol. 3, ed. Ronald V. Clarke, 151–196. Monsey, NY: Criminal Justice Press.

Cornish, Derek B., and Ronald V. Clarke. 2008. The rational choice perspective. In Environmental criminology and crime analysis, ed. Richard Wortley and Lorraine Mazerolle, 21–47. Cullompton: Willan Publishing.

Felson, Marcus. 2008. Routine activity approach. In Environmental criminology and crime analysis, ed. Richard Wortley and Lorraine Mazerolle, 70–77. Cullompton: Willan Publishing.

Financial Services Commission. 2023. Daemyeon pyeonchwihyeong boiseupising-do pihae gujae daesang-e pohamdoemnida [Face-to-face collection voice phishing now covered by victim relief]. Press release, November 16. Seoul: Financial Services Commission.

Financial Services Commission. 2025. Dajung pihae sagi geunjeol daechaek [Comprehensive measures to eradicate multi-victim fraud]. Joint government press reference, July 31. Seoul: Financial Services Commission. https://www.fsc.go.kr/no010101/85039.

Financial Services Commission. 2026a. Boiseupising uisim geumyung·tongsin·susa jeongbo, ASAP-eul tonghae bongyeokjeogeuro gongyudoemnida [Suspicious financial, telecommunications and investigative information on voice phishing to be shared through ASAP]. Press release, August 4. Seoul: Financial Services Commission. https://www.fsc.go.kr/no010101/87474.

Financial Services Commission. 2026b. Jinhwahaneun pisingbeomjoedo domangchil got eopda: Sinjongpising iyong uisim gyejwa georaereul jeuksi chadanhagetseumnida [Immediate restrictions on accounts suspected of use in novel phishing]. Press release, June 30. Seoul: Financial Services Commission. https://www.fsc.go.kr/no010101/87212.

Financial Services Commission. 2026c. On gajogi moin seol myeongjeol, boiseupising yebang haengdong suchigeul gieokhaseyo! [Remember the voice-phishing prevention rules during the Lunar New Year holiday: Ten rules for preventing voice-phishing victimization]. Press release, February 10. Seoul: Financial Services Commission. https://www.fsc.go.kr/no010101/86250.

Financial Supervisory Service. 2025. 2024-nyeon boiseupising pihae hyeonhwang bunseok [Analysis of 2024 voice-phishing damage]. Public statistical release. Seoul: Financial Supervisory Service.

Flyvbjerg, Bent. 2006. Five misunderstandings about case-study research. Qualitative Inquiry 12 (2): 219–245. https://doi.org/10.1177/1077800405284363.

Galis, Vasilis, and Björn Karlsson. 2024. A world of Palantir: Ontological politics in the Danish police's POL-INTEL. Information, Communication & Society 27 (13): 2438–2456. https://doi.org/10.1080/1369118X.2024.2410255.

Haelterman, Harald. 2016. Crime script analysis: Preventing crimes against business. London: Palgrave Macmillan.

Johnson, Shane D. 2024. Identifying and preventing future forms of crimes using situational crime prevention. Security Journal 37: 515–534. https://doi.org/10.1057/s41284-024-00441-5.

Joint Government Ministries. 2023. Boiseupising, ije 112-ro singohaseyo [Voice phishing: Now report via 112]. Press release, September 26. Seoul: Office for Government Policy Coordination.

Joint Government TF. 2026. Beomjeongbu boiseupising daeeung TF chujin seonggwa [Achievements of the pan-governmental voice-phishing response task force]. Press release, May 27. Seoul: Office for Government Policy Coordination.

Korea Internet & Security Agency. 2026. “Deungbon balgeup sido dwaetda” jumin-senteo jeonhwa, pisingil su itseumnida [A call claiming an attempted resident-record issuance may be phishing]. Press release, April 29. Naju: Korea Internet & Security Agency. https://www.kisa.or.kr/402/form?postSeq=2588.

Motie, Soroor, and Bijan Raahemi. 2024. Financial fraud detection using graph neural networks: A systematic review. Expert Systems with Applications 240: 122156. https://doi.org/10.1016/j.eswa.2023.122156.

National Police Agency. 2018. Boiseupising beomjoe-ui jaeguseong, “geu nom moksori”e sokji maseyo! [Reconstructing voice-phishing crime: Do not be deceived by “that voice”]. Press release, May 23. Seoul: National Police Agency. https://www.police.go.kr/user/bbs/BD_selectBbs.do?q_bbsCode=1002&q_bbscttSn=1B000001120299000.

National Police Agency. 2025a. 2024 beomjoe tonggye [2024 crime statistics]. Seoul: National Police Agency.

National Police Agency. 2025b. “Mungorie georeodulgeyo,” sagiui sijagieotda!? [“I’ll leave it on the door handle”: Was that the beginning of the scam?]. Public information card, July 16. Seoul: National Police Agency. https://www.police.go.kr/user/bbs/BD_selectBbs.do?q_bbsCode=1007&q_bbscttSn=20250716135116298.

National Police Agency. 2026a. Pising beomjoe teukbyeol dansok gyeolgwa [Results of the special crackdown on phishing crimes]. Press release, February 6. Seoul: National Police Agency (National Office of Investigation).

National Police Agency. 2026b. Sinjong seukaemgwa-ui jeonjaeng, deo ppallajin daeeung-ui bigyeoreun? [War on new scams: Why has the response become faster?]. Public information

card, July 6. Seoul: National Police Agency. https://www.police.go.kr/user/bbs/BD_selectBbs.do?q_bbsCode=1007&q_bbscttSn=20260706153404862.

Otte, J. Neil, John Beverley, and Alan Ruttenberg. 2022. BFO: Basic Formal Ontology. Applied Ontology 17 (1): 17–43. https://doi.org/10.3233/AO-220262.

Patton, Michael Quinn. 2015. Qualitative research & evaluation methods. 4th ed. Thousand Oaks, CA: Sage.

Smith, Barry, and Werner Ceusters. 2010. Ontological realism: A methodology for coordinated evolution of scientific ontologies. Applied Ontology 5 (3–4): 139–188. https://doi.org/10.3233/AO-2010-0079.

West, Jarrod, and Maumita Bhattacharya. 2016. Intelligent financial fraud detection: A comprehensive review. Computers & Security 57: 47–66. https://doi.org/10.1016/j.cose.2015.09.005.

Whitty, Monica T. 2013. The scammers persuasive techniques model: Development of a stage model to explain the online dating romance scam. British Journal of Criminology 53 (4): 665–684. https://doi.org/10.1093/bjc/azt009.

Yin, Robert K. 2018. Case study research and applications: Design and methods. 6th ed. Thousand Oaks, CA: Sage.

Supplementary Files

This is a list of supplementary files associated with this preprint. Click to download.

- 04SecurityJournalSupplementaryAppendixAv3.3.docx