International Journal of Engineering Research and Modern Education (IJERME)
Impact Factor: 7.018, ISSN (Online): 2455 - 4200
(www.rdmodernresearch.com) Volume 5, Issue 2, 2020

QUANTIFYING DEEPFAKE PAYMENT FRAUD RISK ACROSS CORPORATE TREASURY APPROVAL SYSTEMS

Kannan Vishwanath* & Lloyd Zulu**
* Fellow, Albert Schweitzer International Foundation, Karl-Löwe-Gasse 22/12, A-1120 Wien, Vienna, Austria
** World Christian University, Lusaka, Zambia

Cite This Article: Kannan Vishwanath & Lloyd Zulu, "Quantifying Deepfake Payment Fraud Risk Across Corporate Treasury Approval Systems", International Journal of Engineering Research and Modern Education, Volume 5, Issue 2, Page Number 18-26, 2020.

Copy Right: © IJERME, 2020 (All Rights Reserved). This is an Open Access Article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Abstract:

This analysis examines reported payment impersonation fraud and its implications for interpreting corporate deepfake risk within international financial security debates. A descriptive documentary design analyzes five annual Internet Crime Complaint Center aggregates covering 2014 to 2018, preserving published categories, monetary units, and precision qualifiers. Reported business email compromise complaints increased from 2,417 in 2014 to 7,838 in 2015. Within the combined business email and personal email account compromise category, complaints increased from 12,005 in 2016 to 20,373 in 2018, while reported nominal losses rose from USD 360.51 million to USD 1.30 billion. Category changes restrict interpretation of these observations as a continuous corporate series. The analysis distinguishes recorded complaint volume, financial consequences, and payment exposure, clarifying why aggregate losses cannot directly measure deepfake prevalence or approval effectiveness. This measurement distinction connects behavioral security explanations with the administrative evidence required to evaluate payment controls. The findings inform reporting practices by supporting consistent fraud classifications, explicit exposure denominators, and transaction records linking verification, authorization, intervention, and recovery.

Key Words: Business Email Compromise; Payment Impersonation; Deepfake Fraud; Financial Risk Measurement; Documentary Analysis

1. Introduction:

A payment instruction can appear authentic while directing funds to a fraudulent beneficiary. Corporate treasury operations depend on communication among executives, payment officers, approvers, and financial institutions. Impersonation exploits these relationships by converting apparent authority into an instruction to transfer funds. Synthetic voice introduces an additional source of apparent credibility. Munich Re Specialty (2019) describes a reported incident involving executive voice impersonation and a EUR 220,000 transfer by a UK energy company. The account illustrates a payment fraud mechanism but does not establish its prevalence or quantify the protection provided by corporate controls.

The broader financial consequences of payment impersonation are evident in official complaint records. The Federal Bureau of Investigation, Internet Crime Complaint Center (2019) reported 20,373 business email and email account compromise complaints with approximately USD 1.30 billion in reported losses for 2018. These figures cover a broader category than deepfake fraud and include personal account compromise. Their significance lies in the financial burden recorded within the reporting system rather than an estimate of corporate transaction risk. Distinguishing these interpretations is essential when using aggregate fraud statistics to inform treasury governance.

Behavioral security research explains why formal procedures may not consistently prevent deceptive instructions from producing harmful actions. Johnston and Warkentin (2010) associate protective intentions with perceived threat, response effectiveness, personal capability, and social influence. Bulgurcu et al. (2010) show that security compliance intentions reflect attitudes, normative beliefs, perceived capability, and assessments of compliance consequences. These findings suggest that employees evaluate both the apparent legitimacy of an instruction and the consequences of challenging it. However, neither investigation establishes the effect of treasury approval controls on confirmed deepfake payment outcomes. Their relevance to this analysis is theoretical rather than direct empirical validation.

The conceptual framework distinguishes three protective functions. Identity verification establishes whether the requesting person and payment instruction are authentic. Payment authorization distributes decision authority and requires scrutiny before release. Transaction monitoring identifies unusual characteristics and initiates further review. These functions address different points in the payment process. Their effectiveness may depend on independent information, substantive review, and timely intervention. Repeated reliance on the same compromised communication could instead allow several procedural checks to reproduce one mistaken judgment. These are proposed mechanisms rather than effects estimated from the available records.

The reviewed evidence identifies a measurement gap between reported fraud burden and corporate payment vulnerability. Annual complaint counts do not identify the number of eligible payment requests.

Aggregate losses do not separate confirmed synthetic impersonation from other deception or identify the controls operating when payments were approved. The Joint Task Force Transformation Initiative (2012) distinguishes threats, vulnerabilities, likelihood, and consequences within risk assessment. This distinction explains why reported losses alone cannot establish whether a particular approval arrangement is effective.

This study aims to characterize the available evidence on reported payment impersonation fraud and establish its implications for interpreting corporate deepfake payment risk. The empirical question asks what annual complaint and loss records establish about reported payment fraud and which interpretations require corporate transaction evidence. The objectives are to compare reported complaint volumes, examine financial consequences, and assess comparability across published categories. The three protective functions organize the theoretical interpretation without being presented as estimated predictors.

The analysis uses five annual reporting aggregates covering 2014 to 2018, drawn from official publications released within the permitted literature period. Its unit of analysis is the reporting system year. Descriptive comparison preserves original category labels, nominal monetary units, and numerical precision. The design supports assessment of recorded financial burden rather than causal estimation, corporate risk prediction, or hypothesis testing concerning approval effectiveness.

The contribution is an explicit separation of reported complaint volume, reported financial consequence, and payment exposure. This separation prevents broad fraud categories from being treated as direct observations of deepfake incidents. It also clarifies the evidence required to evaluate verification, authorization, and monitoring. Its international relevance rests on this transferable measurement logic, while numerical conclusions remain bounded by the reporting system and categories examined.

2. Theory, Conceptual Framework, and Hypotheses Development:

This analysis develops a theoretical explanation of how corporate treasury approval controls may constrain deepfake payment fraud. Corporate payments depend on communication among executives, payment officers, approvers, and financial institutions. Attackers can exploit these relationships by presenting fraudulent instructions as legitimate managerial requests. Deepfake impersonation introduces synthetic voice or video into this process, potentially making an instruction appear credible without establishing its authenticity. Munich Re Specialty (2019) describes a reported synthetic voice incident involving executive impersonation and a corporate transfer. This account illustrates the mechanism but does not establish its prevalence or the effectiveness of particular controls.

Corporate treasury approval controls constitute the independent construct. They comprise identity verification, payment authorization, and transaction monitoring. Deepfake payment fraud risk constitutes the dependent construct and concerns the likelihood and financial consequences of successful synthetic impersonation within eligible payment requests. Its proposed indicators are fraudulent payment approval rate, successful fraudulent transfer rate, gross fraud loss per eligible request, net unrecovered loss per eligible request, and repeated successful fraud incidents. These indicators capture different outcomes and are not assumed to form a validated scale.

Protection motivation theory provides a behavioral foundation for the framework. Employees may follow protective procedures when they recognize a threat, believe the recommended response can address it, and consider themselves capable of performing that response. Johnston and Warkentin (2010) find that security intentions depend partly on perceived response effectiveness, personal capability, threat severity, and social influence. Their evidence concerns information security behavior rather than deepfake payment fraud. Its application here therefore supports a theoretical expectation, not an established corporate fraud relationship.

Identity verification establishes whether a payment instruction originates from an authorized person. Its proposed components are independent callback verification, authentication using multiple factors, and executive identity confirmation. The mechanism is evidentiary separation: approval depends on information obtained through an independently established channel rather than solely on the appearance or sound of the original request.

Stronger verification should reduce the probability that synthetic impersonation results in payment approval. This expectation depends on the independence of the verification channel. Calling a number supplied within the suspicious request may reproduce the same deception. Authentication of a system account also does not necessarily establish that the account holder intended a particular payment. Verification must therefore connect the requesting person, the payment details, and the authorization decision.

The Financial Crimes Enforcement Network (2019) identifies compromised payment communications and vulnerable business processes as central features of email compromise fraud. This evidence supports attention to the authenticity of payment instructions, although it does not quantify the effect of identity verification against deepfake attacks. Verification may also impose delays that encourage procedural bypass. The expected protective relationship therefore applies when employees perform the checks and attackers do not control the independent channel.

H1: Stronger identity verification is associated with lower deepfake payment fraud risk when verification uses an independent channel and confirms the specific payment instruction.

Payment authorization governs who may approve a transaction and under which conditions. Its proposed components are separation of duties, dual payment approval, and approval threshold enforcement. These controls distribute decision authority so that one deceived employee cannot independently initiate and release an eligible payment.

The expected mechanism is independent scrutiny. A second approver can question unusual instructions, verify supporting evidence, or identify inconsistencies overlooked by the first employee. The Joint Task Force Transformation Initiative (2013) provides an institutional foundation for separating duties and controlling access within organizational security arrangements. Applying this logic to treasury workflows suggests that authorization controls can interrupt the conversion of impersonation into payment execution. This remains a theoretical extension rather than a demonstrated effect on deepfake fraud.

Additional approval does not necessarily provide additional scrutiny. Approvers may rely on the same fabricated evidence, defer to apparent executive authority, or treat approval as a routine administrative step. Bulgurcu et al. (2010) show that security compliance intentions reflect attitudes, normative beliefs, perceived capability, and assessments of compliance costs. These findings support the expectation that authorization effectiveness depends on employees applying the procedure rather than merely satisfying its formal requirements.

H2: Stronger payment authorization controls are associated with lower deepfake payment fraud risk when approvers assess requests independently and enforce authorization requirements.

Transaction monitoring identifies suspicious payment characteristics and initiates a response before or after execution. Its proposed components are unusual payment detection, beneficiary change verification, and suspicious request escalation. Monitoring examines the transaction itself, including inconsistencies that may remain visible even when an impersonated identity appears credible.

The mechanism connects detection with intervention. An unusual beneficiary, unexpected payment destination, or departure from established payment behavior can trigger verification or temporary suspension. Dempsey et al. (2011) describe continuous monitoring as a process that links information collection, analysis, reporting, and response. This supports the proposed importance of timely escalation, but does not establish that general security monitoring directly reduces deepfake payment losses.

Monitoring can also increase recorded fraud by revealing attempts that previously escaped detection. A higher number of detected incidents may therefore accompany stronger controls without indicating greater underlying risk. False alerts may further weaken attention and delay intervention. The expected negative association concerns successful fraudulent payments and resulting losses, provided that alerts reach authorized staff before funds become irrecoverable.

H3: Stronger transaction monitoring is associated with lower deepfake payment fraud risk when suspicious requests trigger timely verification and intervention.

The conceptual framework position's identity verification, payment authorization, and transaction monitoring as distinct dimensions of corporate treasury approval controls. Their proposed relationships with deepfake payment fraud risk are negative associations. The dimensions describe operational practices rather than interchangeable manifestations of a latent trait. No composite weights or measurement scale are assumed.

The framework also distinguishes fraudulent approval from completed transfer and gross loss from unrecovered loss. Repeated incident counts require adjustment for payment exposure and observation duration before comparisons across corporations are meaningful. The hypotheses permit unsupported or inconclusive results. They remain theoretical propositions because the available aggregate fraud reports do not contain linked corporate controls, confirmed deepfake classifications, and payment exposure denominators.

3. Data:

3.1 Data Sources, Population, and Sample:

This analysis assessed secondary evidence for measuring deepfake payment fraud risk across corporate treasury approval systems during 2010 to 2019. The intended population comprises corporate payment requests processed through identifiable approval workflows. The global numbers of eligible corporations, workflows, and payment requests remain unknown because no verified corporate sampling frame was established.

Nine official Internet Crime Complaint Center annual reports covering reporting years 2011 to 2019 were retrieved. The attempted 2010 report download returned an index page. Separate annual business email compromise figures were not identified in the reviewed text of the retrieved 2011 to 2013 reports.

Source selection was purposive and based on relevance, institutional provenance, and accessibility. It did not constitute probability sampling of corporations or a census of corporate transactions. The accessible numerical unit is a reporting system year, whereas the intended corporate unit is an individual payment request. The Federal Bureau of Investigation (2018) explains that IC3 annual reports aggregate submitted complaints and identify reported crime patterns.

The descriptive subset contains five annual observations covering 2014 to 2018, drawn from publications released within the specified citation window. Reporting year was distinguished from publication year. The Federal Bureau of Investigation (2019) confirms that the report covering 2018 was released the

following April. The report covering 2019 was excluded because its publication falls outside the permitted window.

Table 1: Source Selection and Analytical Sample Availability

Stage	Units	Observations	Selection Basis
Retrieved annual reports	9 reports	9 editions	Reporting years 2011 to 2019
Extracted contextual records	One reporting system	6 annual records	Reporting years 2014 to 2019
Excluded by publication window	One report	1 annual record	Publication outside the permitted window
Retained descriptive subset	One reporting system	5 annual records	Reporting years 2014 to 2018

The accessible evidence provides context for payment impersonation fraud. Munich Re Specialty (2019) describes a reported synthetic voice impersonation involving a UK energy company and a EUR 220,000 transfer. This account illustrates a possible mechanism but provides neither a payment exposure denominator nor an authenticated approval dataset.

3.2 Data Preparation, Measurement, and Quality Control:

Original reports were preserved separately from extracted records. The extraction code converted report text into annual observations and verified the uniqueness of the reporting system and year combination. No corporate matching or merging was performed because corporate identifiers were unavailable. Missing observations were retained with explanatory status fields. No interpolation, imputation, carrying forward, trimming, or winsorization was applied. Reported amounts remained in nominal United States dollars. Amounts expressed in millions were converted to dollar units while preserving their precision qualifiers. No inflation adjustment or currency conversion was performed.

Table 2: Variable Definitions and Measurement Limitations

Variable	Analytical Role	Operational Definition	Unit and Frequency
Reporting year	Temporal identifier	Reference year of the annual report	Calendar year
Source category	Classification	Original BEC or BEC/EAC category	Annual
Complaints	Contextual indicator	Published annual complaint count	Complaints annually
Reported loss	Contextual indicator	Published loss under the source category	Nominal USD annually
Loss qualifier	Quality indicator	Rounded amount, lower bound, or published integer	Annual
Deepfake payment risk	Intended outcome	Successful confirmed deepfake payments relative to eligible exposed requests	Not measured
Approval controls	Intended explanatory measures	Controls operating before each payment request	Not measured

Note. BEC denotes business email compromise. EAC denotes email account compromise. Definitions reflect the retrieved reports and the intended corporate measurement requirements.

Table 3: Retained Annual Contextual Observations

Reporting Year	Published Category	Complaints	Reported Loss in Nominal USD
2014	BEC	2,417	226 million, rounded
2015	BEC	7,838	More than 263 million
2016	BEC/EAC	12,005	360,513,961
2017	BEC/EAC	15,690	676,151,185
2018	BEC/EAC	20,373	1,297,803,489

Note. Data are from the Federal Bureau of Investigation, Internet Crime Complaint Center annual reports published in 2015, 2016, 2017, 2018, and 2019. Physical PDF locations are page 16 for reporting year 2014, page 12 for 2015, pages 19 and 20 for 2016, pages 20 and 21 for 2017, and pages 19 and 20 for 2018. Published precision is preserved. These figures do not measure deepfake fraud separately.

Category changes restrict temporal comparability. The combined BEC/EAC category includes business email compromise and personal email account compromise. The Federal Bureau of Investigation, Internet Crime Complaint Center (2017) presents combined figures while stating that combined tracking begins in 2017. This inconsistency was preserved as a measurement limitation.

No dependent risk variable, explanatory index, moderator, or interaction was constructed. The attachment provides no framework defining these measures, and the retrieved sources lack the required corporate records. No latent measurement model was specified. Factor analysis, composite reliability, and average variance extracted were therefore not applied.

Quality checks addressed provenance, extraction accuracy, observation keys, units, coverage, and category definitions. Means and standard deviations were not pooled across changing categories, rounded amounts, and lower bounds. The annual observations preserve these differences directly.

3.3 Analytical Approach, Identification, and Reproducibility:

The completed analysis is descriptive. It presents published complaint counts, reported losses, and coverage limitations. No corporate panel, regression, moderation model, fixed effects, or causal estimates were produced.

The intended outcome requires confirmed deepfake payment events and an exposure denominator drawn from the same corporate workflows. Evaluation of approval effectiveness additionally requires dated approval configurations, unsuccessful attempts, legitimate payment requests, and relevant confounders. None was retrieved as a linked dataset.

The evidence cannot distinguish changes in fraud occurrence from changes in detection and reporting. The Federal Bureau of Investigation (2019) explains that public complaints inform annual reporting and investigative responses. Complaint totals therefore describe reported activity rather than the probability that an eligible corporate payment request results in fraud.

The reported synthetic voice incident does not resolve this identification problem. Munich Re Specialty (2019) describes an individual transfer and impersonation sequence without providing a comparison group, workflow exposure, or verified counterfactual. The account supports discussion of the mechanism rather than estimation of control effectiveness.

Replication materials preserve original reports, extracted records, source URLs, file checksums, variable definitions, missingness flags, and extraction code. These materials permit reproduction of the contextual tables. Complete revision histories and separate redistribution licences were not verified.

The verified evidence supports descriptive contextual analysis. Retaining the corporate risk objective requires linked payment records, contemporaneous approval logs, documented deepfake classifications, and exposure denominators.

4. Methods:

4.1 Research Design and Analytical Scope:

This analysis employed a descriptive documentary design to examine annual business email compromise complaints and reported financial losses. The research question concerned the patterns observable in official reporting aggregates and the comparability of their underlying categories. The unit of analysis was the reporting system year. The analytical sample comprised five annual observations covering 2014 to 2018, extracted from Internet Crime Complaint Center reports published between 2015 and 2019.

The design distinguished reported complaint volume from reported financial consequences. This distinction reflects the separation of likelihood and impact in organizational risk assessment (Joint Task Force Transformation Initiative, 2012). Complaint counts and loss amounts were interpreted according to their published definitions rather than treated as interchangeable measures of payment vulnerability. The annual reports supplied the empirical basis for this comparison (Federal Bureau of Investigation, Internet Crime Complaint Center, 2015, 2016, 2017, 2018, 2019).

Sources were selected purposively for their institutional provenance, relevance to payment impersonation fraud, and accessible numerical content. Reporting year was distinguished from publication year. The sample therefore represents dated reporting aggregates within the selected publications rather than a probability sample of corporations.

4.2 Data Extraction and Analytical Procedures:

Original PDF reports were preserved separately from the structured extract. Python code and the Poppler utility pdftotext converted source documents into searchable text and extracted the numerical records. Each record contained the reporting year, original category label, complaint count, reported loss, precision qualifier, and physical PDF page location. The reporting system and year combination formed the observation key, which was checked for uniqueness.

Extraction followed the published category definitions. The reports covering 2014 and 2015 presented business email compromise figures, while the reports covering 2016 to 2018 presented a combined business email and email account compromise category (Federal Bureau of Investigation, Internet Crime Complaint Center, 2015, 2016, 2017, 2018, 2019). These labels were retained because the combined category includes personal account compromise and therefore changes the scope of the observed aggregate.

Monetary observations were expressed in nominal United States dollars. Amounts published in millions were converted to dollar units while preserving their precision qualifiers. The figure for 2014 was recorded as rounded, and the figure for 2015 was recorded as exceeding the stated amount. This treatment preserved the

distinction between a rounded observation, a lower bound, and a published integer amount (Federal Bureau of Investigation, Internet Crime Complaint Center, 2015, 2016).

Descriptive comparison examined the direction of annual changes in complaint counts and reported losses. Interpretation distinguished the business email compromise observations from the combined category observations. The annual table retained the original figures and qualifiers, allowing readers to assess variation without obscuring changes in coverage or numerical precision. The combined category observations were interpreted using the complaint and loss tables in the corresponding annual editions (Federal Bureau of Investigation, Internet Crime Complaint Center, 2017, 2018, 2019).

4.3 Quality Assurance and Reproducibility:

Quality assurance addressed provenance, extraction accuracy, observation keys, units, coverage, and classification consistency. Extracted observations were checked against the relevant source passages and tables. Physical PDF page locations were recorded to support independent verification. Original documents, extracted text, structured records, source URLs, and file checksums were preserved as separate replication materials.

The category review identified a comparability issue in the report covering 2016. That edition presents combined business email and email account compromise figures while stating that combined tracking begins in 2017 (Federal Bureau of Investigation, Internet Crime Complaint Center, 2017). The extract preserved the published label and documented the inconsistency. Temporal interpretation consequently remained sensitive to classification boundaries.

Coverage records distinguished unavailable observations from genuine zeros. Precision flags distinguished exact published integer amounts from rounded figures and lower bounds. These controls ensured that numerical presentation remained consistent with the source evidence. In particular, the qualified monetary observations were interpreted according to their original wording rather than assigned unsupported precision (Federal Bureau of Investigation, Internet Crime Complaint Center, 2015, 2016).

The replication package contains the extraction code, software requirements, original documents, variable definitions, coverage flags, and structured numerical records. The code rebuilds the extract and checks observation key uniqueness. Together, these procedures support a reproducible description of reported payment fraud while maintaining alignment between the reporting categories, measurement units, and substantive interpretation.

5. Findings:

This analysis examines annual complaints and reported financial losses associated with business email compromise. It identifies patterns within the available reporting categories while preserving differences in classification and numerical precision. The evidence supports descriptive conclusions about reported fraud rather than estimates of corporate deepfake risk.

5.1 Reported Fraud Complaints:

The descriptive dataset comprises five annual reporting aggregates covering 2014 to 2018. Each observation represents a reporting system year rather than an individual corporation or treasury approval system.

Table 4: Annual Reported Complaints and Financial Losses

Reporting Year	Published Category	Complaints	Reported Financial Loss in Nominal USD
2014	Business email compromise	2,417	226 million, rounded
2015	Business email compromise	7,838	More than 263 million
2016	Business email and email account compromise	12,005	360,513,961
2017	Business email and email account compromise	15,690	676,151,185
2018	Business email and email account compromise	20,373	1,297,803,489

Note. Data are from the Federal Bureau of Investigation, Internet Crime Complaint Center (2015, 2016, 2017, 2018, 2019). Physical PDF locations are page 16, page 12, pages 19 and 20, pages 20 and 21, and pages 19 and 20, respectively. Amounts retain their published precision. The combined category includes personal email account compromise and does not isolate deepfake incidents.

The Federal Bureau of Investigation, Internet Crime Complaint Center (2015) reported 2,417 business email compromise complaints for 2014. The following annual edition reported 7,838 complaints for 2015. These observations indicate greater recorded complaint volume within the business email compromise category. They do not establish changes in victimization probability because the reports provide no denominator of eligible businesses or payment requests.

Within the published combined category, complaints increased from 12,005 in 2016 to 15,690 in 2017 and 20,373 in 2018. The Federal Bureau of Investigation, Internet Crime Complaint Center (2017, 2018, 2019) therefore documents successive increases in reported complaint volume. Reporting participation and classification changes remain possible contributors to this pattern.

5.2 Reported Financial Losses:

The financial evidence indicates substantial nominal losses within the published categories. The Federal Bureau of Investigation, Internet Crime Complaint Center (2015, 2016) reported a rounded USD 226 million for 2014 and more than USD 263 million for 2015. Their different precision conventions prevent treatment as exact comparable totals.

The combined category recorded USD 360,513,961 in 2016, USD 676,151,185 in 2017, and USD 1,297,803,489 in 2018. Both complaint volume and reported losses increased across these observations (Federal Bureau of Investigation, Internet Crime Complaint Center, 2017, 2018, 2019). However, these aggregates cannot determine whether losses increased because of more incidents, larger individual losses, changes in reporting composition, or several factors operating together.

The highest complaint count and reported loss in the retained records occurred in 2018. This finding concerns published reporting aggregates. It does not identify the highest corporate fraud rate or demonstrate weaker payment approval controls.

5.3 Interpretation of the Available Evidence:

The empirical contribution is a documented comparison of complaint volume and reported financial losses. The records show increasing reported amounts within the displayed categories while identifying a classification boundary between business email compromise and the combined business and personal account category.

The Federal Bureau of Investigation, Internet Crime Complaint Center (2017) presents combined figures while stating that combined tracking begins in 2017. The analysis therefore preserves the published labels and avoids estimating a single growth rate across all five observations.

The available variables support descriptive tabulation rather than estimation of corporate approval effectiveness. Identity verification, payment authorization, transaction monitoring, and confirmed deepfake exposure were not measured in these records. The proposed control relationships consequently remain theoretical propositions rather than tested empirical findings.

The evidence establishes substantial reported financial consequences associated with payment impersonation categories. The defensible contribution is the comparison of those recorded outcomes, with conclusions restricted to the definitions and coverage of the published data.

6. Discussion:

Increasing reported losses do not, by themselves, demonstrate increasing fraud risk. Table 4 records successive increases in complaints and nominal losses within the published combined category, but neither measure incorporates total payment exposure. The contribution of this analysis is therefore a distinction between reported financial burden and transaction risk. The Joint Task Force Transformation Initiative (2012) treats risk assessment as an evaluation of threats, vulnerabilities, likelihood, and consequences rather than a comparison of loss totals alone. This distinction changes the interpretation of the observed pattern: higher reported losses establish greater recorded financial consequences, but cannot identify whether payment requests became more vulnerable. The analysis supports a descriptive interpretation without introducing regression coefficients, significance levels, or equation references that were not produced.

The theoretical mechanisms concern how employees interpret apparent authority and apply verification procedures, but Table 4 does not measure these processes. A plausible pathway connects executive impersonation to perceived legitimacy, procedural bypass, and payment execution. Siponen and Vance (2010) show that employees can rationalize violations of information security policies, providing a behavioral explanation for why formal controls may not translate into consistent compliance. Applied to treasury decisions, this suggests that urgency or perceived managerial authority could encourage exceptions to verification requirements. This is a theoretical interpretation, not an observed mediation effect. The conceptual implication is that control adoption and control execution should be treated as distinct explanatory variables rather than assumed to be equivalent.

The available evidence permits decomposition of the analytical problem rather than decomposition of estimated effects. Complaint volume, reported financial loss, and payment exposure represent different quantities. Their separation prevents an increase in recorded complaints from being interpreted automatically as greater loss severity or weaker authorization. Table 4 also separates business email compromise from the broader combined category, showing why classification must precede temporal comparison. No channel can be ranked as dominant because identity verification, authorization, and monitoring were not jointly observed. The theoretical contribution is a measurement framework that distinguishes the occurrence of a reported event, its financial consequence, and the population exposed to it. These distinctions establish what a future explanation must account for without assigning unsupported shares to competing mechanisms.

The classification changes reveal a structural challenge in translating administrative fraud records into corporate governance evidence. Reporting systems organize complaints for operational purposes, while analysis of treasury controls requires payment requests linked to dated approval decisions. Combining business and personal account categories changes the meaning of the observed total even when the numerical series appears

continuous. This matters because apparent temporal growth may reflect changes in the reporting population alongside changes in criminal activity. The analysis therefore redirects attention from the size of the dataset to alignment among the reporting category, unit of observation, and intended claim. For decision makers, aggregate totals can inform awareness and resource planning, while evaluation of approval procedures requires records of verification, exceptions, rejected requests, and completed transfers.

International evidence illustrates why payment fraud trajectories cannot be generalized across instruments or jurisdictions. The European Central Bank (2018) reported a decline in total card fraud in 2016 alongside an increase in fraud involving payments made without presenting a card. That pattern differs from the rising combined complaint and loss totals displayed in Table 4, but the difference cannot be attributed to stronger European controls because the datasets cover different payment mechanisms and reporting populations. The comparison instead demonstrates the importance of instrument specific exposure denominators and consistent classifications. The practical implication is to report fraud amounts alongside eligible transaction volumes and distinguish attempted, prevented, completed, and recovered payments. Future comparative analysis should test whether controls influence these separate stages, allowing theoretical explanations to address both fraud prevention and detection without treating reported totals as interchangeable measures of security performance.

7. Conclusion and Implications:

Financial losses can command attention while leaving the underlying probability of fraud unmeasured. This analysis shows that published complaint records document substantial financial consequences but require careful interpretation before informing corporate security decisions. Its contribution separates recorded events, reported monetary consequences, and the population exposed to fraudulent instructions. That distinction redirects attention from aggregate growth toward the evidence required to assess payment vulnerability, consistent with the risk assessment approach described by the Joint Task Force Transformation Initiative (2012). The proposed protective mechanisms explain how independent confirmation, distributed scrutiny, and timely intervention could interrupt deception, but the descriptive results do not establish their separate or combined effects. Behavioral evidence also indicates that procedural requirements and employee execution should remain analytically distinct (Bulgurcu et al., 2010; Johnston & Warkentin, 2010). Managers can apply this insight by recording verification actions, approval exceptions, rejected requests, completed transfers, and recoveries within a common transaction record. Policymakers can support comparable reporting through consistent definitions and explicit payment denominators. Operational improvements should connect suspicious instructions to documented decisions and outcomes rather than rely on complaint totals as performance measures. This approach can strengthen accountability and make fraud prevention efforts more assessable across financial systems.

The available records provide a foundation for descriptive comparison and a direction for further inquiry. Their annual aggregation, changing categories, and absence of corporate exposure denominators motivate transaction-based datasets linking requests, approval procedures, incident classifications, and recoveries. Future research should distinguish suspected from confirmed synthetic impersonation and retain unsuccessful attempts alongside legitimate payments. Longitudinal corporate records could examine whether procedural changes precede changes in outcomes. International comparisons should harmonize payment instruments and reporting definitions before comparing performance. Such extensions would permit direct evaluation of the proposed mechanisms and establish where their applicability depends on institutional conditions.

References:

1. Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. MIS Quarterly, 34(3), 523-548. https://doi.org/10.2307/25750690
2. Dempsey, K., Chawla, N. S., Johnson, A., Johnston, R., Jones, A. C., Orebaugh, A., Scholl, M., & Stine, K. (2011). Information security continuous monitoring for federal information systems and organizations (NIST Special Publication 800-137). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-137
3. European Central Bank. (2018). Fifth report on card fraud. https://www.ecb.europa.eu/press/card fraud/html/ecb.cardfraudreport201809.en.html
4. Federal Bureau of Investigation. (2018, May 7). 2017 internet crime report released. https://www.fbi. gov/news/stories/2017-internet-crime-report-released-050718
5. Federal Bureau of Investigation. (2019, April 22). 2018 IC3 report released. https://www.fbi.gov/news/ stories/ic3-releases-2018-internet-crime-report-042219
6. Federal Bureau of Investigation, Internet Crime Complaint Center. (2015). 2014 internet crime report. https://www.ic3.gov/AnnualReport/Reports/2014_IC3Report.pdf
7. Federal Bureau of Investigation, Internet Crime Complaint Center. (2016). 2015 internet crime report. https://www.ic3.gov/AnnualReport/Reports/2015_IC3Report.pdf

8. Federal Bureau of Investigation, Internet Crime Complaint Center. (2017). 2016 internet crime report. https://www.ic3.gov/AnnualReport/Reports/2016_ic3report.pdf
9. Federal Bureau of Investigation, Internet Crime Complaint Center. (2018). 2017 internet crime report. https://www.ic3.gov/AnnualReport/Reports/2017_IC3Report.pdf
10. Federal Bureau of Investigation, Internet Crime Complaint Center. (2019). 2018 internet crime report. https://www.ic3.gov/AnnualReport/Reports/2018_IC3Report.pdf
11. Financial Crimes Enforcement Network. (2019, July 16). Updated advisory on email compromise fraud schemes targeting vulnerable business processes (Advisory FIN-2019-A005). https://www.fincen.gov/resources/advisories/fincen-advisory-fin-2019-a005
12. Johnston, A. C., & Warkentin, M. (2010). Fear appeals and information security behaviors: An empirical study. MIS Quarterly, 34(3), 549-566. https://doi.org/10.2307/25750691
13. Joint Task Force Transformation Initiative. (2012). Guide for conducting risk assessments (NIST Special Publication 800-30, Revision 1). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-30r1
14. Joint Task Force Transformation Initiative. (2013). Security and privacy controls for federal information systems and organizations (NIST Special Publication 800-53, Revision 4). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-53r4
15. Munich Re Specialty. (2019, September 26). Deepfake voice generation software presents a new frontier for fraudsters. https://www.munichre.com/specialty/global-markets-uk/en/insights/cyber/deepfake-voice-generation-software.html
16. Siponen, M., & Vance, A. (2010). Neutralization: New insights into the problem of employee information systems security policy violations. MIS Quarterly, 34(3), 487-502. https://doi.org/10.2307/25750688