

E-Commerce Performance and Criminal Law Liability Risk in Digital Markets: Evidence from Jordan

Mohammad Airout

Faculty of Law, Department of Law, Middle East University, Amman, Jordan

Abstract. This research study examines the associations between cyber-fraud exposure, criminal liability risk, service governance, and perceived e-commerce performance within a purposive sample of Jordanian e-commerce firms. Using signaling theory and information processing theory, data from 386 surveyed Jordanian e-commerce firms were analyzed using partial least squares structural equation modeling (PLS-SEM) in SmartPLS software. Compliance readiness is positively associated with platform accountability, which is positively associated with consumer trust. Consumer trust is the strongest positive correlate of perceived e-commerce performance in the sampled firms. The mediation results show that compliance readiness carries the associations of cyber-fraud exposure and criminal liability risk with performance, while platform accountability and consumer trust indicate how governance readiness is statistically linked to performance. The moderation analysis indicates that the positive association between cyber-fraud exposure and compliance readiness is stronger when criminal liability risk is high. The study contributes analytical evidence from a purposive sample by showing how fraud-related risk, compliance capability, accountable platform processes, and trust are jointly associated with perceived performance among surveyed Jordanian e-commerce firms. The findings should not be interpreted as representative sector-wide estimates.

Keywords: e-commerce; cyber-fraud; compliance; accountability; trust; performance.

1. Introduction

E-commerce now operates as a platform-based service system in which payment infrastructures, digital interfaces, seller verification routines, complaint-handling channels, and information transparency jointly shape service performance. In Jordan, this service-system perspective is increasingly important. The Central Bank of Jordan's National Strategy for Electronic Payments in Jordan 2023-2025 emphasizes the development of modern electronic payment systems and the need for a secure and reliable payment environment (Central Bank of Jordan, 2023). Jordan Payments and Clearing Company reported that transactions processed through its systems reached 224.62 million in 2024, with a total value of 79.95 billion JOD (Jordan Payments and Clearing Company, 2025). The Ministry of Digital Economy and Entrepreneurship reported, based on the 2024 household ICT usage and access survey, that individual internet use in Jordan reached 95.6%, while daily internet use reached 94.8% (Ministry of Digital Economy and Entrepreneurship, 2026).

However, in such circumstances, the consumers will make purchases without direct physical examination of products and without complete understanding of the sellers. Hence, trust of clients can be defined by factors like secure payment options provided, identification of the sellers, accurate representation of products, refund policies and complaint management. Extensive academic research demonstrates that trust and perceived risks are core concepts of transaction acceptance in electronic commerce environment (Pavlou, 2003; Gefen et al., 2003). Moreover, recent studies confirm that trust and consumer perception in general still remain directly dependent on platform design, quality of service provision, level of transparency, and online risk management practices (Quintus et al., 2024; Singh et al., 2024).

Meanwhile, fraud exposure introduces additional complexity for the service systems involved. Potential risks in e-commerce include false purchases, account impersonation, improper usage of funds received, misleading listings, misleading advertising content, and disputes related to the evidence and delivery records. Based on some research papers related to fraud detection, sellers' behaviors and the behavior of customers can be identified as some clear markers indicating fraud activity, and as such, all of their behaviors should be continuously monitored in order to reduce this issue (Alba et al., 2025; Zhang et al., 2025). Therefore, in terms of digital governance, the above risks become much broader than just technical issues to overcome. Instead, they become risks of documentation, accountability, and risks of exposure.

Criminal liability risk is considered an important element of digital governance in the Jordanian e-commerce environment, as presented in the current survey. Criminal liability risk refers to risks in relation to the fact that the seller, manager, employee, or any other intermediary involved in e-commerce may be accused of illegal activities or investigated in terms of possible fraud committed in the online space. This aspect does not refer merely to a doctrinal issue, as criminal liability can emerge as a governance pressure in a particular digital environment and may be associated with greater compliance readiness and performance-relevant governance conditions among surveyed firms (Eni et al., 2024; Shukri et al., 2024). In continuation with this idea, this paper examines compliance readiness as a key information processing capacity, platform accountability as a key governance indicator, consumer trust as a perceived service outcome, and performance as a reported service-system outcome.

Although there is a vast amount of literature regarding online shopping, platform governance, and social commerce, several aspects still require further exploration. Specifically, many researchers discuss adoption and purchase intentions of consumers or features of websites, whereas criminal liability risk remains neglected despite the fact that many e-commerce cases may end up in court trials. At the same time, empirical research has yet to explore the link between exposure to cyber-frauds, criminal liability risk, compliance readiness, platform accountability, consumer trust, and perceived e-commerce performance among surveyed Jordanian e-commerce firms. Therefore, this research proposes and tests

a PLS-SEM model using evidence from a purposive sample of surveyed firms rather than a representative sector-wide sample.

2. Literature Review

2.1 Theoretical foundation and study positioning

This study blends together both theories of signaling and information processing. Signaling theory posits that in the presence of information asymmetry, individuals base their judgments about unobservable quality, reliability, or integrity on observable signals (Spence, 1973). The same applies in e-commerce since the buyer cannot verify the seller, internal control system, or processes involved in the resolution of disputes. These observable signals of governance become important because they are the basis for reducing uncertainties. This line of thought is supported by seminal studies on trust formation in e-commerce environments which emphasize the role of credible signals that lower perceived risks (Gefen et al., 2003; Pavlou, 2003).

The information processing theory offers another angle from which one can understand what organizations do when faced with uncertainties. According to Galbraith (1974) and Daft & Lengel (1986), greater levels of equivocality and uncertainty require richer information, greater coordination, and more formalized processes. Within the context of digital transactions, greater risk of cyber-fraud and associated liabilities mean higher needs for verification, monitoring, documentations, complaint processing, and evidence retention. Therefore, the capability of compliance readiness could be understood as the means of managing information processing needs related to fraud and service system risks (Taqa, 2025).

Compliance readiness represents the organizational capability required to satisfy those needs, whereas platform accountability becomes the external governance signal created by that capability. Consumer trust refers to customers' perceptions of those signals, while perceived e-commerce performance represents the reported service-system outcome in the surveyed firms.

2.2 E-Commerce Risk, Cyber-Fraud Exposure, and Criminal Liability Risk

E-commerce increases the reach of marketing and flexibility of services but at the same time, introduces unique risk conditions. On the buyer side, they are exposed to uncertainties related to the vendor, potential abuse of payments, misinformation, and disputes after purchase, whereas for businesses, there might be concerns with regard to fraudulent orders, manipulation, chargeback type of risks, and lack of evidence. Both empirical studies examining social commerce and shopping risk in an e-commerce context and theoretical analysis of legal and ethical considerations around e-commerce support the conclusion that uncertainties associated with identity, security, and platform reliability are still among the major factors that stand in the way of trust in digital transactions (Al-Adwan & Yaseen, 2023; Alrawad et al., 2023; Wahab et al., 2023; Channak et al., 2023).

For the purpose of this study, cyber-fraud risk reflects the degree to which organizations are exposed to the problem of fraud incidents or risks associated with the process of digital sale, including fake accounts, fraudulent transactions, abuse of payments, and manipulation of communication. According to fraud detection and prevention literature, such types of risks occur quite regularly and can be recognized based on behavior and transaction data. Thus, they must be treated as governance challenges, rather than purely operational issues (Alba et al., 2025; Zeng et al., 2025; Zhang et al., 2025).

Criminal liability risk is a narrower term than general legal risk. In essence, it refers to the perception of the likelihood that fraud-related incidents, manipulation or misleading practices, insufficient verification, poor evidence management, or deficiencies in consumer protection mechanisms will make organization representatives exposed to the risk of criminal complaints, investigation, and potential liability. Legal literature examining the responsibilities of online

marketplaces and the problem of consumer protection justifies that it is important to distinguish the two risks in question (Fairgrieve et al., 2024; Filatova-Bilous, 2023; Mallet et al., 2025).

For the purposes of clarifying the boundaries of criminal liability risk construct, it is essential to differentiate it from cyber-risk, compliance risk, regulatory risk, and reputational risk. Specifically, the former is related to technical exposure, the latter to failure to adhere to the procedures or rules, and the former to the change of regulations or their increased stringency. Reputation risk refers to stakeholders' perceptions. Legal risk is a general umbrella concept, while criminal liability risk is a particular governance challenge.

2.3 Compliance Readiness and Platform Accountability

Compliance readiness entails the degree to which an e-commerce business has the routines, documentation, controls, and internal capability required for meeting legal, procedural, consumer protection, and cybersecurity risks. In the context of digital services, such compliance readiness involves record keeping, verification routines, secure data handling, complaint reporting, documentation for refunds, surveillance for any suspicious activity, documentation of any digital evidence, among other aspects. From the perspective of information processing, such routines assist the business in absorbing and organizing risk-related information amid uncertainty.

Platform accountability entails the visible governance routines through which the business or the platform signals its responsibility and manages transactions in question. This involves providing transparent seller information, monitoring suspicious activities, assigning responsibilities, articulating transaction terms, addressing customer complaints, and providing returns/dispute routines that are accessible to the buyer. As suggested by signaling theory, such practices are meaningful since they allow customers to get cues regarding whether the service system is credible and reliable. Recent studies concerning platform governance also stress that visible governance routines, together with monitoring and community rules, are related to platform participants' behaviors (Li et al., 2024; Zhao et al., 2023).

Although they are related, platform accountability and compliance readiness are distinguishable concepts. While the latter pertains to the capabilities that an e-commerce business possesses internally, the former is concerned with signals that customers can observe and understand. More specifically, compliance readiness involves verifying whether the firm has the capability while platform accountability involves whether the firm provides evidence regarding its capability and responsibility to the customer.

To sharpen these boundaries, this study treats the three constructs as operating at different levels of the governance-service chain. Compliance readiness refers to internal organizational capacity; platform accountability refers to outwardly visible practices through which that capacity is communicated to users; and consumer trust refers to the evaluative confidence attributed to customers. Although all three constructs are positive governance-related constructs and may appear connected in practice, the model separates them as internal capability, external accountability signal, and perceived trust outcome.

2.4 Consumer Trust and E-Commerce Performance

Consumer trust has emerged as one of the most consistently identified antecedents of transaction success in online settings. Previous foundational research demonstrates that trust minimizes perceived risks and fosters intentions for engaging in online transactions that lack any possibility of direct inspection and personal interaction (Pavlou, 2003; Gefen et al., 2003). Recent systematic review studies and empirical analyses also confirm that security, privacy, high-quality service provision, and responsiveness encourage consumers to develop trustful beliefs regarding their use of e-commerce sites (Kuen et al., 2023; Quintus et al., 2024; Singh et al., 2024).

Based on this theoretical logic, it follows that platform accountability should be positively associated with consumer trust due to the reduction in ambiguity and uncertainty associated with such factors as reliability, justice, and protection after the transaction. Previous studies exploring complaint

management practices, customer service, websites' assurances, and trust formation mechanisms in C2C settings also support such associations because transparent service recovery procedures, privacy protection measures, and high-quality response practices may foster increased trust and repurchase intentions (Istanbulluoglu & Sakman, 2024; Mayayise, 2024; Rodriguez-Priego et al., 2023; Saxena & Thakur, 2024).

Performance in e-commerce is viewed here as an outcome resulting from the functioning of a service system and measured through sales, customer retention rates, reputation building, continuity, and growth in the market. Earlier research shows that platform-based capabilities, commitment, trust, and customer engagement have a close relationship with performance and repurchase outcomes within the context of e-commerce activities performed by SMEs (Ballerini et al., 2023; Hanaysha et al., 2025; Herzallah & Al-Sharaf, 2025).

2.5 Criminal Liability Risk as a Digital Service Governance Pressure

One might think about criminal liability risk from the perspective of both sides – as a liability burden that reduces the motivation for expansion and generates uncertainties while shifting attention from growth towards regulation and correction or alternatively, as a pressure on digital governance that is likely to prompt firms to adopt new processes and measures to formalize and improve information processing practices.

Accordingly, under one interpretation, liability risk implies worse performance, since companies are likely to become more cautious, incur additional compliance costs and act under increased reputation pressure. In another interpretation, liability risk can be considered as a pressure for better digital governance, which may manifest itself as adoption of more advanced documentation and verification practices, proper handling of customer complaints, and evidence collection and preservation measures. The logic of regulatory pressure and deterrence suggests that the higher the likelihood of sanctions or investigations and the more serious they are expected to be, the more incentives there are for adopting formal procedures, improving controls and reducing exposure to risks related to evidence.

Recent scholarship on internet intermediaries' liability, platform responsibility, and electronic consumer protection supports the latter viewpoint by demonstrating that legal accountability is increasingly seen as a component of platform governance (Aade, 2025; Law, 2025; Sahak et al., 2026; Sarabdeen, 2026). This dual framework appears relevant for Jordanian e-commerce settings such as those examined in this study, where growing connectivity and electronic payment penetration may make transaction failure more noticeable and hence give rise to perceived criminal liability risks.

2.6 Gap Analysis

Three gaps support the necessity of developing the proposed model. First, the majority of studies about e-commerce focus on adoption, purchase intention, customer experience, or platform-related characteristics, leaving criminal liability risk as a factor affecting governance understudied. Second, research on platform accountability and trust does not sufficiently link these constructs with upstream fraud exposure and compliance capability. Third, while many studies about e-commerce in emerging economies discuss digital-commerce growth, they do not provide enough information about how firms transform their risk perception into accountable service processes (Oreqat, 2021).

It is necessary to emphasize that these gaps are associated with the nature of the problem under discussion. As was noted in the literature dedicated to the topics of e-commerce trust and digital governance, service quality, information transparency, and secure information exchange should be considered as essential elements in the research, yet no study examines the association of fraud-related exposure and criminal liability risk with compliance capability, platform accountability, trust, and performance (Eni et al., 2024; Shukri et al., 2024).

2.7 Hypotheses Development

The increased visibility of exposure linked to fraud-related threats would make it easier for managers to draw the inference that inadequate controls, poor documentation, or fraud-prone transactions may lead to some adverse consequences. Under the information processing theory, the higher level of fraud exposure signals increases the salience of uncertainty and the importance of understanding the potential consequences of the exposure. The relationship between the two variables is hence expected to be positive.

H1: Cyber-fraud exposure is positively associated with criminal liability risk.

As the cyber-fraud exposure increases, there are increased chances that the firm will formalize its verification processes, its record keeping, and complaint handling mechanisms, all of which are information processing techniques in response to heightened uncertainty. Therefore, cyber-fraud exposure should be positively related to compliance readiness.

H2: Cyber-fraud exposure is positively associated with compliance readiness.

The increased risk of criminal liabilities should be positively associated with compliance readiness. Risk-governance or regulatory pressure theory suggests that businesses facing high risks in terms of being exposed to criminal complaints, investigations, or sanctions are more likely to formalize their responsibilities, preserve records of their operations, and document transactions to prove their due diligence and minimize exposure. Hence, salience of criminal liability is not only related to uncertainty but also to governance pressure.

H3: Criminal liability risk is positively associated with compliance readiness.

Compliance readiness is expected to be positively related to platform accountability since the internal capabilities of the business facilitate credible governance. Firms with the capability to carry out verification, documentation, and complaint handling may be better positioned to communicate transaction details, monitor suspicious activity, and preserve the evidence. These activities are expected to be associated with stronger platform accountability and, in turn, consumer trust.

H4: Compliance readiness is positively associated with platform accountability.

H5: Platform accountability is positively associated with consumer trust.

Since consumers place a high level of trust on the platform, there will be no hesitance regarding the purchase, which will lead to greater repeat purchases and better performance for the business. At the same time, compliance readiness and platform accountability may also have direct associations with performance due to dispute reduction and continuity. On the other hand, the liability risk may have a negative association with performance in that it is viewed as uncertainty and burden.

H6: Consumer trust is positively associated with e-commerce performance.

H7: Compliance readiness is positively associated with e-commerce performance.

H8: Platform accountability is positively associated with e-commerce performance.

H9: Criminal liability risk is negatively associated with e-commerce performance.

The model also anticipates indirect pathways. If cyber-fraud exposure and criminal liability risk are associated with stronger compliance readiness, and compliance readiness is associated with performance directly and through accountable platform processes, then governance capability should mediate these relationships statistically. In addition, platform accountability and consumer trust should carry part of the association between compliance readiness and performance.

H10: Compliance readiness mediates the positive association between cyber-fraud exposure and e-commerce performance.

H11: Compliance readiness mediates the positive association between criminal liability risk and e-commerce performance.

H12: Platform accountability and consumer trust sequentially mediate the association between compliance readiness and e-commerce performance.

H13: Consumer trust mediates the association between platform accountability and e-commerce performance.

Finally, criminal liability risk may intensify the cyber-fraud exposure-compliance readiness association. From a regulatory-pressure and deterrence perspective, the same level of fraud exposure may be associated with stronger compliance readiness when managers believe that weak controls or poor documentation could escalate into formal complaint, investigation, or sanction. Perceived liability is greater and hence increases the perceived costs of non-action, increasing the probability that firms will consider fraud alerts as indicators that need governance discipline.

H14: The relationship between cyber fraud and compliance preparedness is positively moderated by criminal liability threat, such that the relationship is stronger when criminal liability threat is high.

3. Methodology

This research uses a quantitative explanatory research design to examine the associations among cyber-fraud experience, perceived criminal liability risk, compliance readiness, accountability, consumer trust, and perceived e-commerce performance among surveyed Jordanian e-commerce firms. This type of design focuses on prediction and is appropriate to examine several direct, indirect, and moderating relationships between the constructs. Because the design is cross-sectional, based on perceptual survey data, and drawn from a purposive sample, the empirical paths, mediation results, and moderation result are interpreted as statistical associations within the sampled firms rather than evidence of causal process effects or representative sector-wide patterns.

The target population comprised Jordanian enterprises undertaking e-commerce operations. These include online stores, social commerce enterprises, digital marketplace enterprises, logistics-based e-commerce enterprises, financial service providers and SMEs utilizing websites, apps, or social media sites for digital sale of products and services. E-commerce enterprise constitutes the unit of analysis and the survey was directed to one knowledgeable person within each e-commerce business enterprise. The survey was designed for owners, managers, compliance staff, accounts and finance staff, customer service representatives or operations staff knowledgeable about digital selling, fraud, complaints handling and compliance processes.

A purposive sampling approach was used owing to lack of availability of a representative sample of Jordanian e-commerce businesses in the country. Eligible firms were identified from observable online-selling activity visible on business websites, marketplace storefronts, and social-media selling pages, followed by targeted researcher outreach to active e-commerce businesses in commercially active Jordanian areas. The electronic questionnaire link was circulated in a targeted manner through direct business contacts and online business networks used by e-commerce sellers; it was not released as an unrestricted public survey. Because some firms were reachable through more than one route and outreach records were maintained at the overall circulation level rather than by route, exact channel-specific contact counts could not be reconstructed retrospectively. The questionnaire instructions requested that one knowledgeable representative respond on behalf of each business. Where multiple submissions appeared to refer to the same business, the most complete usable response was retained and the others were excluded. Incomplete survey forms, obvious straight-line responding, and repeated organization responses were screened out during data collection. In all, 520 survey forms were distributed, and only 386 usable survey forms were collected after data cleaning. Because the study relied on non-probability purposive sampling and targeted electronic circulation, the findings should be interpreted as analytically informative evidence from the surveyed firms rather than statistically representative of all Jordanian e-commerce firms or of the sector as a whole. Formal non-response bias testing was not feasible under this design because the circulation process did not involve a closed sampling frame with trackable wave-response information, and this limitation is acknowledged explicitly. Accordingly, references to the Jordanian e-commerce context in the findings should be read

as referring to the purposive sample and comparable firms, not as national prevalence or sector-wide performance estimates.

The sample size was adequate for PLS-SEM within the analytical sample. The largest number of arrows pointing to an endogenous construct in the model is four (e-commerce performance), which implies a minimum of 40 observations under the ten-times rule. In addition, for four predictors, $\alpha = 0.05$, power = 0.80, and a medium effect size, the required minimum sample is well below the final usable sample. Therefore, 386 responses comfortably exceeded common minimum requirements for the structural model tested. This adequacy supports model estimation, but it does not imply statistical representativeness of the whole Jordanian e-commerce sector.

Table 1. Sample Profile of Jordanian E-Commerce Businesses

Category	Classification	Frequency	Percentage
Business type	Online retail	124	32.1%
	Social commerce seller	89	23.1%
	Digital marketplace/platform	54	14.0%
	Logistics-supported e-commerce	47	12.2%
	Payment-related service provider	32	8.3%
	Other online business	40	10.3%
Respondent position	Owner/partner	102	26.4%
	Manager	96	24.9%
	Accounting/finance employee	71	18.4%
	Compliance/legal-related employee	45	11.7%
	Marketing/customer service employee	72	18.6%
Business size	Micro	91	23.6%
	Small	151	39.1%
	Medium	104	26.9%
	Large	40	10.4%
Years of e-commerce activity	Less than 2 years	83	21.5%
	2–5 years	169	43.8%
	6–10 years	96	24.9%
	More than 10 years	38	9.8%

The questionnaire was developed from the conceptual model and adapted to the Jordanian e-commerce context. The cyber-fraud exposure items were informed by the e-commerce fraud and online risk literature. Criminal liability risk items were designed to gauge the extent of perception toward criminal complaints and investigations due to poor verification, deceptive practices, poor evidence preservation, or failure to protect consumers. The compliance readiness items encompassed documentation, verification, dispute resolution, and evidence preservation capacity. Platform accountability items included seller visibility, monitoring, complaints management, and responsibility allocation. Two constructs measuring consumer trust and e-commerce performance were used to measure consumer confidence and service systems' results, respectively. The statement was reformulated in terms of online shopping, social commerce, platform sales, and financial services practices in Jordan.

In order to minimize construct overlapping in the instrument, the survey questions were tailored to represent the different levels. Compliance readiness items covered internal documentation, verification,

procedures, and knowledge about the company's policies and procedures, while platform accountability items entailed seller/platform visibility and customer-oriented procedures, and consumer trust items involved reliability, fairness, transparency, and trustworthiness. As mentioned above, the study recruited only one person per company to represent their knowledge, and thus it is expected that the perception could still produce some positive-valence overlapping between governance constructs.

For purposes of clarifying the measurement instrument, an expert panel comprising five experts in business laws, accounting, e-commerce, digital governance, and research methodology was contacted to evaluate the clarity, content validity, and contextual relevance of the survey. Following minor modifications, pilot testing was conducted on a sample of 30 respondents employed by Jordanian e-commerce firms. No problems emerged regarding the wording and format, and all constructs attained a Cronbach's alpha value exceeding 0.70. Each construct was evaluated using a five-point Likert scale from strongly disagree at 1 to strongly agree at 5. The resulting questionnaire included 29 items presented in Appendix A.

Table 2. Measurement Constructs and Operational Definitions

Construct	Operational Definition	Number of Items
Cyber-Fraud Exposure	The extent to which e-commerce businesses face risks related to online fraud, fake orders, impersonation, digital payment misuse, and deceptive online transactions.	5
Criminal Liability Risk	The perceived risk that e-commerce activities may create criminal liability exposure for sellers, platforms, managers, or responsible employees.	5
Compliance Readiness	The ability of the business to comply with legal, procedural, documentation, consumer protection, and cyber-risk requirements.	5
Platform Accountability	The extent to which online platforms or sellers apply verification, monitoring, complaint-handling, refund, and evidence-preservation mechanisms.	5
Consumer Trust	The degree to which customers perceive online sellers or platforms as reliable, secure, transparent, and legally accountable.	4
E-Commerce Performance	The perceived improvement in online sales, customer retention, reputation, operational continuity, and digital market growth.	5

The type of analysis used in this case was performed using Partial Least Squares Structural Equation Modeling using the SmartPLS software. This particular choice of approach was made due to the fact that this is a study with predictions, as well as many variables and mediations. Indeed, recent studies have shown that PLS-SEM is appropriate for predictive studies in business, especially in complex model settings (Gudergan et al., 2025; Ringle et al., 2023). The analysis followed two stages. First, the measurement model was assessed through indicator loadings, Cronbach's alpha, rho_A, composite reliability, average variance extracted (AVE), and HTMT discriminant validity. Second, the structural model was assessed through path coefficients, t-values, p-values, R², Q², effect sizes (f²), indirect effects, moderation, and common-method diagnostics. Bootstrapping with 5,000 resamples was used to test the significance of the direct, indirect, and moderating associations.

Common method bias was addressed procedurally by assuring confidentiality, using neutral wording, separating constructs within the questionnaire, and avoiding identifiable business or customer information. It was also assessed statistically through Harman's single-factor test and full collinearity VIF. Participation was voluntary. No personal names, transaction-level identifiers, legal-case details, or account details were collected, and all findings are reported in aggregate form.

4. Results

4.1 Measurement Model Assessment

The measurement model was first assessed through indicator loadings. As shown in Table 3, all item loadings range from 0.776 to 0.892, exceeding the common 0.70 benchmark. The indicators therefore provide adequate representation of their respective latent constructs. Establishing reliable measurement is particularly important here because the model combines risk, compliance, accountability, trust, and performance dimensions that must remain empirically separable before the structural associations are interpreted.

Table 3. Measurement Model Results

Construct	Item	Loading	Decision
Cyber-Fraud Exposure	CFE1	0.821	Retained
	CFE2	0.864	Retained
	CFE3	0.839	Retained
	CFE4	0.807	Retained
	CFE5	0.776	Retained
Criminal Liability Risk	CLR1	0.845	Retained
	CLR2	0.872	Retained
	CLR3	0.831	Retained
	CLR4	0.808	Retained
	CLR5	0.789	Retained
Compliance Readiness	CR1	0.854	Retained
	CR2	0.881	Retained
	CR3	0.836	Retained
	CR4	0.812	Retained
	CR5	0.847	Retained
Platform Accountability	PA1	0.823	Retained
	PA2	0.861	Retained
	PA3	0.842	Retained
	PA4	0.819	Retained
	PA5	0.798	Retained
Consumer Trust	CT1	0.874	Retained
	CT2	0.892	Retained
	CT3	0.861	Retained
	CT4	0.833	Retained
	CT5	0.852	Retained
E-Commerce Performance	EP1	0.856	Retained
	EP2	0.882	Retained
	EP3	0.871	Retained
	EP4	0.838	Retained
	EP5	0.852	Retained

The reliability and convergent validity test was done using Cronbach's alpha, rho_A, composite reliability, and average variance extracted (AVE). The values of Cronbach's alpha range from 0.874 to 0.902, while the values of rho_A range from 0.881 to 0.907. The values of composite reliability range from 0.912 to 0.934, while the values of AVE range from 0.676 to 0.749.

Table 4. Reliability and Convergent Validity

Construct	Cronbach's α	rho_A	CR	AVE	Decision
Cyber-Fraud Exposure	0.881	0.889	0.912	0.676	Accepted
Criminal Liability Risk	0.889	0.896	0.917	0.688	Accepted
Compliance Readiness	0.902	0.907	0.927	0.716	Accepted
Platform Accountability	0.874	0.881	0.916	0.687	Accepted
Consumer Trust	0.881	0.886	0.923	0.749	Accepted
E-Commerce Performance	0.897	0.903	0.934	0.739	Accepted

The test for the discriminant validity was conducted through the HTMT approach. As is evident from Table 5 below, the HTMT ratio is below 0.85, indicating that there is empirical discrimination among the variables. This is particularly critical for distinguishing between the cyber-fraud threat and criminal liability threat, as well as compliance preparedness, platform responsibility, and consumer trust (Ahmad et al., 2023).

Table 5. Discriminant Validity (HTMT)

Pair	HTMT	Decision
CFE $\leftrightarrow$ CLR	0.742	Established
CFE $\leftrightarrow$ CR	0.668	Established
CFE $\leftrightarrow$ PA	0.631	Established
CFE $\leftrightarrow$ CT	0.594	Established
CFE $\leftrightarrow$ EP	0.612	Established
CLR $\leftrightarrow$ CR	0.701	Established
CLR $\leftrightarrow$ PA	0.673	Established
CLR $\leftrightarrow$ CT	0.658	Established
CLR $\leftrightarrow$ EP	0.681	Established
CR $\leftrightarrow$ PA	0.722	Established
CR $\leftrightarrow$ CT	0.756	Established
CR $\leftrightarrow$ EP	0.781	Established
PA $\leftrightarrow$ CT	0.739	Established
PA $\leftrightarrow$ EP	0.768	Established
CT $\leftrightarrow$ EP	0.812	Established

Apart from the HTMTs, the conceptual borders between the three governance constructs have been taken into consideration. Compliance readiness is the capability of an organization to adhere to processes and maintain proper documentation. Platform accountability refers to governance practices that are externally observable and communicated by the seller or platform to the user. Consumer trust is the perceived level of trust in the dependability, fairness, transparency, and accountability of the

service delivery system. The constructs are empirically plausible and conceptually distinct, despite the tentative interpretation due to common perspective of measurement.

4.2 Structural Model Assessment

After setting up the measurement model, a further analysis was done concerning the structural model based on direct relations, explanation, prediction validity, effect size, indirect relation, and moderation. Table 6 presents the estimates for the direct path coefficients. There exists a positive relation between cyber-fraud exposure and criminal liability risk, as supported by H1. This suggests that firms reporting higher exposure to cyber-fraud, including fake orders, impersonation, fraudulent payments, and deception, are also likely to report stronger perceived criminal liability risk in cyber-governance (Al-Muntasir, 2022).

Cyber-fraud exposure has a positive correlation with compliance readiness, as stated in H2, and criminal liability risk is positively related to compliance readiness, as stated in H3. These relationships are consistent with stronger verification, documentation, handling of complaints, and preservation of evidence in the process of compliance. Compliance readiness is positively related to platform accountability, as stated in H4, and platform accountability, in turn, is positively related to consumer trust, as stated in H5. It corresponds to the proposed theory of information processing and signaling.

There is a significant positive relationship between consumer trust and e-commerce performance, as stated in H6. Furthermore, it is the strongest positive relationship in the model. Compliance readiness and platform accountability are positively related to performance, as stated in H7 and H8. However, criminal liability risk is negatively related to e-commerce performance, as stated in H9. These results are interpreted as statistical associations within the cross-sectional model.

Table 6. Structural Model Results

Hypothesis	Path	Beta	t-value	p-value	Decision
H1	CFE → CLR	0.611	13.002	< 0.001	Supported
H2	CFE → CR	0.482	8.991	< 0.001	Supported
H3	CLR → CR	0.317	5.776	< 0.001	Supported
H4	CR → PA	0.538	10.224	< 0.001	Supported
H5	PA → CT	0.564	11.337	< 0.001	Supported
H6	CT → EP	0.603	12.114	< 0.001	Supported
H7	CR → EP	0.241	3.882	< 0.001	Supported
H8	PA → EP	0.198	3.104	0.002	Supported
H9	CLR → EP	-0.146	2.442	0.015	Supported

Table 7 shows the explanatory quality and predictive relevance of the model within the sample. Specifically, the model explains 37.3%, 52.8%, 28.9%, 31.8%, and 70.1% of the variation in criminal liability risk, compliance readiness, platform accountability, consumer trust, and perceived e-commerce performance among the surveyed firms, respectively. The Q² values of all dependent variables are positive.

Table 7. R² and Predictive Relevance

Construct	R ²	Q ²	Interpretation
Criminal Liability Risk	0.373	0.251	Moderate
Compliance Readiness	0.528	0.367	Moderate-High
Platform Accountability	0.289	0.194	Moderate
Consumer Trust	0.318	0.226	Moderate
E-Commerce Performance	0.701	0.482	Substantial

Effect-size estimates are shown in Table 8. Cyber-fraud exposure shows a large f^2 contribution to criminal liability risk; compliance readiness shows a large f^2 contribution to platform accountability; platform accountability shows a large f^2 contribution to consumer trust; and consumer trust shows a large f^2 contribution to e-commerce performance. Smaller but still meaningful f^2 contributions appear for compliance readiness, platform accountability, and criminal liability risk on performance.

Table 8. Effect Size

Path	f^2	Interpretation
CFE → CLR	0.596	Large
CFE → CR	0.281	Medium
CLR → CR	0.142	Small–Medium
CR → PA	0.412	Large
PA → CT	0.471	Large
CT → EP	0.522	Large
CR → EP	0.094	Small
PA → EP	0.071	Small
CLR → EP	0.048	Small

4.3 Mediation Results

The mediation results are reported in Table 9. Cyber-fraud exposure has a significant positive indirect association with e-commerce performance through compliance readiness, supporting H10. Criminal liability risk also has a significant positive indirect association with performance through compliance readiness, supporting H11. These findings indicate that risk-related pressures may be statistically linked to more constructive performance pathways when they are examined through governance capability.

The sequential mediation from compliance readiness to performance through platform accountability and consumer trust is significant, supporting H12. The indirect association of platform accountability with performance via consumer trust is equally important, which supports H13. The above findings indicate that platform accountability and consumer trust are essential downstream statistical pathways through which governance preparedness is associated with commercial significance.

Table 9. Mediation Results

Hypothesis and Indirect Path	Beta	t-value	p-value	Decision
H10: CFE → CR → EP	0.116	3.228	0.001	Significant
H11: CLR → CR → EP	0.076	2.614	0.009	Significant
H12: CR → PA → CT → EP	0.183	4.992	< 0.001	Significant
H13: PA → CT → EP	0.340	8.221	< 0.001	Significant

4.4 Moderation Result

The moderation analysis tested whether the relationship between cyber fraud experience and compliance readiness varies according to the level of criminal liability risk. The interaction variable is positive and significant, thus supporting H14. In other words, the positive relation between cyber fraud experience and compliance readiness is stronger when criminal liability risk is high.

This is the coefficient that is used in making Figure 1, where we have the simple slope plotted graphically depending on the various circumstances. The graph clearly indicates that there is a steep slope linking cyber fraud experience and compliance readiness only when the criminal liability risks are high.

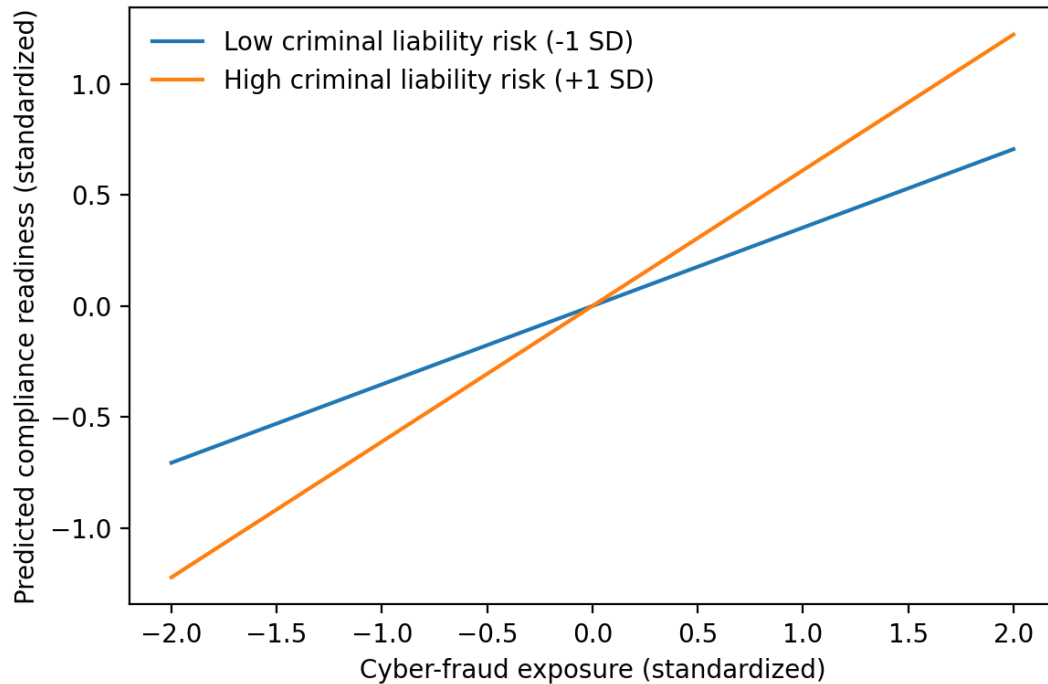


Fig.1 : Standardized simple-slope illustration of the moderating role of criminal liability risk

The figure indicates that the positive association between cyber-fraud exposure and compliance readiness is steeper among businesses perceiving higher criminal liability risk. In practical terms, the same increase in fraud-related exposure is associated with a larger compliance-readiness difference when managers believe that the consequences may extend beyond service failure into formal criminal exposure.

Table 10. Moderation Effect

Hypothesis and Interaction	Beta	t-value	p-value	Decision
H14: CFE x CLR → CR	0.129	2.533	0.012	Significant moderation

4.5 Common Method Bias

Common method bias was assessed using Harman's single-factor test and full collinearity VIF. As shown in Table 11, Harman's single-factor result is 36.2%, below the common 50% threshold, and the full collinearity VIF is 2.81, below the conservative 3.3 threshold. These results suggest that common method bias is not a severe threat, although, as discussed later, it cannot be ruled out completely in a single-source perceptual survey design.

Table 11. Common Method Bias

Test	Result	Decision
Harman's single-factor	36.2%	No serious issue
Full collinearity VIF	2.81	No serious issue

Overall, the results support the proposed digital service governance model within the purposive sample. Cyber-fraud exposure is associated with stronger perceived criminal liability risk and compliance readiness. Criminal liability risk is associated negatively with perceived performance directly but positively with governance readiness. Compliance readiness is associated with stronger platform accountability, which in turn is associated with stronger consumer trust and perceived performance. The model therefore supports the interpretation that risk awareness, information-processing capability, visible accountability, and trust are jointly linked to perceived e-commerce performance among the surveyed Jordanian firms, not that they describe the entire sector (Othman, 2025).

5. Discussion

Findings from the purposive sample support an interpretation of surveyed Jordanian e-commerce firms from the perspective of digital service governance. Firstly, cyber-fraud exposure has a positive association with criminal liability risk and compliance readiness. As expected, the finding aligns with the information processing approach because firms exposed to such threats may report greater need for verification and monitoring to ensure the operation of the service system. Therefore, there is an indication that fraud exposure does not remain a technical problem among the surveyed firms. Managers in this sample also recognize that it poses a governance challenge which may have legal repercussions.

Secondly, a positive association exists between compliance readiness and platform accountability. In this case, firms with high capability to collect data, verify information, and maintain evidence may be better able to communicate important platform characteristics, such as complaint handling procedures and seller information. Importantly, consumers cannot inspect the information control measures implemented by sellers online, which means that they can only rely on observable indicators. In this regard, the proposed theoretical relationship between accountability and consumer trust is consistent with the information asymmetry assumption.

Thirdly, consumer trust is strongly associated with perceived e-commerce performance among the surveyed Jordanian firms. Jordan's wider payment and internet-use indicators provide relevant context for interpreting this pattern, but the empirical result itself refers only to the sampled firms. Consumers often encounter issues with seller identification, accurate descriptions, delivery services, and dispute resolution (Central Bank of Jordan, 2023; Jordan Payments and Clearing Company, 2025; Ministry of Digital Economy and Entrepreneurship, 2026). Thus, accountability assumes extra significance because visible signs of trustworthiness may act as substitutes for personal contact.

Fourthly, the proposed study makes another important contribution to the literature on digital service governance. Namely, it highlights the paradoxical character of criminal liability risk in relation to performance. On the one hand, there is a negative relationship which suggests that liability concerns are associated with lower perceived business performance. On the other hand, criminal liability risk is positively associated with compliance readiness and has a positive indirect association with performance through compliance readiness. This suggests that firms with higher perceived risks may also report stronger governance capacity to cope with cyber-fraud exposure.

Finally, the moderation result offers additional insights into the role of criminal liability risk in digital service governance. Namely, the study found a significant interaction between the two variables, indicating a stronger conditional association between fraud exposure and compliance readiness when liability risk is higher. This is an important finding because it suggests that companies do not report the same compliance-readiness pattern under the same level of fraud exposure. Such variation seems to depend on whether the threat is evaluated as serious enough to escalate into a crime or not.

In conclusion, the discussion presented above supports the view that perceived e-commerce performance among the surveyed Jordanian firms is associated with factors beyond adoption, price, and reach. The findings imply that one needs to consider the relationship between cyber fraud risk,

governance capacity, accountability cues, and trust while assessing performance in the selected e-commerce environment. The above findings should be viewed as evidence based on samples rather than a representation of performance of e-commerce in Jordan.

6. Implications

The findings can be interpreted as a useful governance structure for the surveyed companies and similar electronic commerce companies, acknowledging that the sample used is purposive rather than representative of the industry.

Prevention controls. The firms dealing with e-commerce need to upgrade themselves with regard to seller and buyer verification, safeguarding payment checks, documentation of the transaction process, access controls, and training of employees in fraud prevention and evidence preservation. These will make it clearer before problems arise, allowing for better understanding of any signs of fraud.

Detection controls. Organizations should monitor abnormal purchase patterns, failed payments, repeated categories of complaints, inconsistencies in accounts, and other suspicious activity related to digital commerce. Detection procedures should be coupled with proper escalation procedures so that any fraud-related signals receive due attention in an appropriate manner. As seen from the findings, organizations with high levels of cyber-fraud exposure also report greater compliance preparedness. Therefore, quality detection mechanisms may be relevant to a company's response to its risks.

Response controls. A company needs to develop appropriate measures for managing customer complaints, issuing refunds, implementing service recovery strategies, escalation to upper management levels, dealing with any data breaches, and saving the digital evidence. In light of the associations reported in this study, the presence of properly developed response strategies may enable an organization to cope with its burden and reduce further reputational damage.

Trust-building controls. Platforms and merchants need to give visibility to their governance signals to customers. Transparent seller identification, clear transaction terms, easy access to complaint channels, easy-to-find information about returns and refunds, as well as the dispute resolution progress, can help consumers evaluate whether this particular service operates fairly and responsibly. Platform accountability, a factor positively correlated with consumer trust and performance, means treating trust-building actions as governance activities.

From the perspective of policymakers and regulators in Jordan, the above findings should be treated as analytical evidence from a purposive sample rather than representative sector-wide estimates. They may still be useful for identifying governance issues that deserve attention in comparable e-commerce contexts, particularly where firms face similar fraud, documentation, and trust challenges. Relevant areas include seller identification, evidentiary preservation, complaint management, consumer redress, and collaboration with digital payment providers, while remaining consistent with the national agenda related to digital payments and connectivity (Central Bank of Jordan, 2023; Jordan Payments and Clearing Company, 2025).

Using evidence from surveyed firms, this research adds to the body of knowledge related to e-commerce by advancing criminal liability risk as a governance concept that may be associated with both performance burden and governance pressure in comparable digital commerce settings.

7. Limitations and Future Research

There are a number of limitations in this study. First, the cross-sectional design restricts inference about causation, and so these findings need to be considered from the standpoint of association rather than causation. Second, non-probability purposive sampling means that generalization based on statistical reasoning must be limited, and the results should not be read as a representative profile of the entire Jordanian e-commerce sector, as sector-wide performance estimates, or as evidence of prevalence across all Jordanian digital markets. In particular, given the overlapping targeted electronic routes used

for the survey, as well as the retention of outreach counts only at the total circulation level and not route-specifically, the actual counts by channel type cannot be reestablished. Third, given that the data is obtained at the firm-level from individual respondents, issues of social desirability, perceptual inflation, and common-source bias cannot be definitively controlled for despite various procedural and statistical measures. Fourth, this study uses perception of criminal liability risks instead of actual legal cases or enforcement or transaction-level incident reporting. Fifth, since this model is constrained in nature, omitted variable and reciprocal causality issues may arise. Sixth, because compliance readiness, platform accountability, and consumer trust are all positively valenced governance-related constructs, some conceptual proximity may remain despite acceptable HTMT results and the boundary definitions provided above.

Further research might address the limitations mentioned above through longitudinal studies, business-consumer matched databases, industry-specific samples, cross-national comparison in different digital environments with varied regulatory settings, etc. Another interesting direction to explore is whether marketplace, social commerce, and payment platform types respond to liability concerns via different governance preparations. Objective incident, complaint, and platform log data could be useful as well.

8. Conclusion

In this study, the relationship between exposure to cyber-fraud, criminal liability risk perception, and compliance readiness on the one hand, and platform accountability and consumer trust on the other, as well as their relationship to perceived e-commerce performance among the sampled firms, was explored using the theoretical lens of signaling theory and information processing.

Findings from the purposive sample show that cyber-fraud exposure positively relates to criminal liability risk, and criminal liability risk positively relates to compliance readiness, but negatively relates to perceived e-commerce performance directly. Compliance readiness positively relates to platform accountability, and platform accountability positively relates to consumer trust. Consumer trust is the strongest positive correlate of perceived e-commerce performance among the surveyed firms. The indirect and moderation findings indicate that liability pressure may have an indirect positive association with performance when it is linked with stronger reported governance readiness. Thus, the contribution of this study is its sample-based evidence that criminal liability risk is a two-way factor in the surveyed digital-commerce context because it may be negatively associated with perceived performance directly while being positively associated with compliance readiness and indirectly associated with performance through governance-related pathways. These conclusions should not be interpreted as representative findings for the whole Jordanian e-commerce sector.

References

- Aade, L. (2025). The regulation of social media commerce under the DSA: A consumer protection perspective. *Computer Law & Security Review*, 59, Article 106181. <https://doi.org/10.1016/j.clsr.2025.106181>
- Ahmad, A. K., Nahar, H. M., & Manajreh, M. M. N. (2023). Effect of social media on shaping the agenda of the communicator in the Jordanian TV channels. *Middle East Journal of Communication Studies*, 3(2), 1–40. <https://doi.org/10.71220/2585-003-002-003>
- Al-Adwan, A. S., & Yaseen, H. (2023). Solving the product uncertainty hurdle in social commerce: The mediating role of seller uncertainty. *International Journal of Information Management Data Insights*, 3(1), Article 100169. <https://doi.org/10.1016/j.jjime.2023.100169>

Alba, M. C., Moreira, M. A. L., Favero, L. P., & dos Santos, M. (2025). E-commerce sellers clustering to detect fraud risk on commercial dates. *Procedia Computer Science*, 266, 110-117. <https://doi.org/10.1016/j.procs.2025.08.014>

Al-Muntasir, M. (2022). The phenomenon of information flow from traditional and new media about the Corona pandemic from the perspective of newly graduated media professionals in Yemen. *Middle East Journal of Communication Studies*, 2(2), 7–25. <https://doi.org/10.71220/2585-002-002-005>

Alrawad, M., Lutfi, A., Alyatama, S., Al Khattab, A., Alsoboa, S. S., Almaiah, M. A., Ramadan, M. H., Arafa, H. M., Ahmed, N. A., Alsyouf, A., & Al-Khasawneh, A. L. (2023). Assessing customers' perception of online shopping risks: A structural equation modeling-based multigroup analysis. *Journal of Retailing and Consumer Services*, 71, Article 103188. <https://doi.org/10.1016/j.jretconser.2022.103188>

Ballerini, J., Herhausen, D., & Ferraris, A. (2023). How commitment and platform adoption drive the e-commerce performance of SMEs: A mixed-method inquiry into e-commerce affordances. *International Journal of Information Management*, 72, Article 102649. <https://doi.org/10.1016/j.ijinfomgt.2023.102649>

Central Bank of Jordan. (2023). National strategy for electronic payments in Jordan (2023-2025). https://www.cbj.gov.jo/ebv4.0/root_storage/en/eb_list_page/national_strategy_for_e-payments1.pdf

Channak, Z. M., Alkhateeb, A., Saleh, E., Aldeeb, H., & Alsharif, S. (2023). Business ethics in e-commerce: Legal challenges and opportunities. *Access to Justice in Eastern Europe, Special Issue*, 101-116. <https://doi.org/10.33327/AJEE-18-6S007>

Daft, R. L., & Lengel, R. H. (1986). Organizational information requirements, media richness and structural design. *Management Science*, 32(5), 554-571. <https://doi.org/10.1287/mnsc.32.5.554>

Eni, Y., Princes, E., Hidayat, D., Zulaykha, A., Gunawan, A., & Jason. (2024). Investigating e-service quality, ease of use, trust and satisfaction in Indonesian e-commerce platforms. *Journal of Logistics, Informatics and Service Science*, 11(5), 292-301. <https://doi.org/10.33168/JLISS.2024.0517>

Fairgrieve, D., Busch, C., Buyuksagis, E., Garrett, Z., Straetmans, G., Karaikos, A., Linley, R., Markou, C., & Paterson, J. (2024). Product liability and online marketplaces: Comparison and reform. *International and Comparative Law Quarterly*, 73, 477-504. <https://doi.org/10.1017/S0020589324000046>

Filatova-Bilous, N. (2023). Online platforms and new challenges for modern law on e-commerce. *Problems of Legality*, 162, 312-329. <https://doi.org/10.21564/2414-990X.162.284666>

Galbraith, J. R. (1974). Organization design: An information processing view. *Interfaces*, 4(3), 28-36. <https://doi.org/10.1287/inte.4.3.28>

Gefen, D., Karahanna, E., & Straub, D. W. (2003). Trust and TAM in online shopping: An integrated model. *MIS Quarterly*, 27(1), 51-90. <https://doi.org/10.2307/30036519>

Gudergan, S. P., Moisescu, O. I., Radomir, L., Ringle, C. M., & Sarstedt, M. (2025). Special issue editorial: Advanced partial least squares structural equation modeling applications in business research. *Journal of Business Research*, 188, Article 115087. <https://doi.org/10.1016/j.jbusres.2024.115087>

Hanaysha, J. R., Ramadan, H. I., & Alhyasat, K. M. K. (2025). Exploring the impact of customer reviews, website quality, perceived service quality, and product assortment on online purchase intention: The mediating role of trust. *Telematics and Informatics Reports*, 19, Article 100236. <https://doi.org/10.1016/j.teler.2025.100236>

- Herzallah, F., & Al-Sharafi, M. A. (2025). Mitigating seller uncertainty in social commerce platforms by exploring pre-purchase customer-seller signals. *Digital Business*, 5(1), Article 100116. <https://doi.org/10.1016/j.digbus.2025.100116>
- Istanbulluoglu, D., & Sakman, E. (2024). Successful complaint handling on social media predicts increased repurchase intention: The roles of trust in company and propensity to trust. *European Management Journal*, 42(1), 11-22. <https://doi.org/10.1016/j.emj.2022.06.004>
- Jordan Payments and Clearing Company. (2025). End-of-year systems report 2024. https://www.jopacc.com/sites/default/files/2025-03/end_of_year_systems_report_2024_en.pdf
- Kuen, L., Westmattmann, D., Bruckes, M., & Schewe, G. (2023). Who earns trust in online environments? A meta-analysis of trust in technology and trust in provider for technology acceptance. *Electronic Markets*, 33, Article 61. <https://doi.org/10.1007/s12525-023-00672-1>
- Law, S. (2025). Effective enforcement of the Online Safety Act and Digital Services Act: Unpacking the compliance and enforcement regimes of the UK and EU's online safety legislation. *Journal of Media Law*, 16(2), 263-300. <https://doi.org/10.1080/17577632.2025.2459441>
- Li, W., Sun, C., Li, Y., & Ertz, M. (2024). Effects of business to business e-commerce platform-governance mechanisms on seller firms' performance. *Research in International Business and Finance*, 67, Article 102121. <https://doi.org/10.1016/j.ribaf.2023.102121>
- Mallet, P., Nassar, H., Abdijabar, Z., & Flayyih, N. (2025). Legal protection of the consumer on social media platforms: A comparative study between UAE and Egypt. *Information & Communications Technology Law*. <https://doi.org/10.1080/13600834.2025.2537513>
- Mayayise, T. O. (2024). Investigating factors influencing trust in C2C e-commerce environments: A systematic literature review. *Data and Information Management*, 8(1), Article 100056. <https://doi.org/10.1016/j.dim.2023.100056>
- Ministry of Digital Economy and Entrepreneurship. (2026, April 16). Ministry of Digital Economy and Entrepreneurship announces results of the 2024 household ICT usage and access survey. https://www.modee.gov.jo/En/NewsDetails/Ministry_of_Digital_Economy_and_Entrepreneurship_Announces_Results_of_the_2024_Household_ICT_Usage_and_Access_Survey
- Othman, M. (2025). Evolving financial practices in family enterprises: The impact of generational dynamics on digital transformation in Jordan. *Investment Management & Financial Innovations*, 22(2), 141–154. [https://doi.org/10.21511/imfi.22\(2\).2025.12](https://doi.org/10.21511/imfi.22(2).2025.12)
- Orekat, A. (2021). The degree of satisfaction of Facebook users about its features, usage motives and achieved gratifications: An applied study on students of the Faculty of Mass Communication at the Middle East University. *Middle East Journal of Communication Studies*, 1(1), 7–35. <https://doi.org/10.71220/2585-001-001-001>
- Pavlou, P. A. (2003). Consumer acceptance of electronic commerce: Integrating trust and risk with the technology acceptance model. *International Journal of Electronic Commerce*, 7(3), 101-134. <https://doi.org/10.1080/10864415.2003.11044275>
- Quintus, M., Mayr, K. M., Hofer, K. M., & Chiu, Y.-T. (2024). Managing consumer trust in e-commerce: Evidence from advanced versus emerging markets. *International Journal of Retail & Distribution Management*, 52(10/11), 1038-1056. <https://doi.org/10.1108/IJRDM-10-2023-0609>
- Ringle, C. M., Sarstedt, M., Sinkovics, N., & Sinkovics, R. R. (2023). A perspective on using partial least squares structural equation modelling in data articles. *Data in Brief*, 48, Article 109074. <https://doi.org/10.1016/j.dib.2023.109074>

- Rodriguez-Priego, N., Porcu, L., Prados Pena, M. B., & Crespo Almendros, E. (2023). Perceived customer care and privacy protection behavior: The mediating role of trust in self-disclosure. *Journal of Retailing and Consumer Services*, 72, Article 103284. <https://doi.org/10.1016/j.jretconser.2023.103284>
- Sahak, S., Rajamanickam, R., & Hassan, M. S. (2026). Liability of internet intermediaries and legal challenges: A comprehensive systematic review. *Quality & Quantity*, 60, 2435-2457. <https://doi.org/10.1007/s11135-025-02344-y>
- Sarabdeen, J. (2026). E-consumers: A critical legal analysis of consumer protection laws. *Social Sciences & Humanities Open*, 13, Article 102685. <https://doi.org/10.1016/j.ssaho.2026.102685>
- Saxena, C., & Thakur, P. (2024). Mediating role of trust and privacy concerns between web assurance mechanism and purchase intention of online products. *Telematics and Informatics Reports*, 16, Article 100177. <https://doi.org/10.1016/j.teler.2024.100177>
- Shukri, M., Goyal, S. B., & Singh, D. (2024). A blockchain-based framework for secure information exchange in digital governance systems using proof of resource availability. *Journal of Logistics, Informatics and Service Science*, 11(4), 21-48. <https://doi.org/10.33168/JLISS.2024.0402>
- Singh, N., Misra, R., Quan, W., Radic, A., Lee, S.-M., & Han, H. (2024). An analysis of consumers' trusting beliefs towards the use of e-commerce platforms. *Humanities and Social Sciences Communications*, 11, Article 899. <https://doi.org/10.1057/s41599-024-03395-6>
- Spence, M. (1973). Job market signaling. *The Quarterly Journal of Economics*, 87(3), 355-374. <https://doi.org/10.2307/1882010>
- Taqa, S. B. A. (2025). The mediating role of remote communication on the relationship between electronic human resource management practices and organizational performance in Iraqi commercial banks. *Middle East Journal of Communication Studies*, 5(1), 1–52. <https://doi.org/10.71220/2585-005-001-001>
- Wahab, F., Khan, I., Kamontip, Hussain, T., & Amir, A. (2023). An investigation of cyber attack impact on consumers' intention to purchase online. *Decision Analytics Journal*, 8, Article 100297. <https://doi.org/10.1016/j.dajour.2023.100297>
- Zeng, Q., Lin, L., Jiang, R., Huang, W., & Lin, D. (2025). NNEnsLeG: A novel approach for e-commerce payment fraud detection using ensemble learning and neural networks. *Information Processing & Management*, 62(1), Article 103916. <https://doi.org/10.1016/j.ipm.2024.103916>
- Zhang, Z., Yin, H., Rao, S. X., Yan, X., Wang, Z., Liang, W., Zhao, Y., Shan, Y., Zhang, R., Lin, Y., & Jiang, J. (2025). Identifying e-commerce fraud through user behavior data: Observations and insights. *Data Science and Engineering*, 10, 24-39. <https://doi.org/10.1007/s41019-024-00275-6>
- Zhao, L., Xu, Y., & Xu, X. (2023). The effects of trust and platform innovation characteristics on consumer behaviors in social commerce: A social influence perspective. *Electronic Commerce Research and Applications*, 60, Article 101284. <https://doi.org/10.1016/j.elerap.2023.101284>

Appendix A. Survey Measurement Items

All items were measured on a five-point Likert scale (1 = strongly disagree; 5 = strongly agree).

Cyber-Fraud Exposure (CFE)

CFE1. Our business is exposed to fake orders or suspicious online transactions.

CFE2. Our business faces risks related to impersonation or fake customer/seller accounts.

CFE3. Unauthorized payment use is a concern in our online transactions.

CFE4. Deceptive or misleading transaction attempts occur in our e-commerce operations.

CFE5. Cyber-fraud incidents create operational or reputational risks for our business.

Criminal Liability Risk (CLR)

CLR1. Fraud-related incidents in e-commerce may expose our business to criminal complaints or investigations.

CLR2. Weak verification or documentation may create criminal liability risk for responsible employees or managers.

CLR3. Misleading online advertisements or product information may create criminal liability exposure.

CLR4. Failure to protect customer or payment information may increase criminal liability risk.

CLR5. Poor handling of complaints, refunds, or digital evidence may increase legal or criminal-risk exposure.

Compliance Readiness (CR)

CR1. Our business maintains reliable records of online transactions and customer communications.

CR2. Our business applies verification procedures for relevant customer, seller, or payment information.

CR3. Our business has clear procedures for complaints, refunds, and dispute handling.

CR4. Our business preserves digital evidence when fraud, payment misuse, or disputes occur.

CR5. Employees involved in e-commerce activities understand relevant compliance and legal-risk procedures.

Platform Accountability (PA)

PA1. Our online selling channel provides clear information about seller identity and transaction terms.

PA2. Our online selling channel monitors suspicious activity and fraud-related signals.

PA3. Customer complaints are handled through clear and timely procedures.

PA4. Refund, return, and dispute-resolution procedures are transparent to customers.

PA5. Responsibilities for documentation, complaint handling, and evidence preservation are clearly assigned.

Consumer Trust (CT)

CT1. Customers perceive our online business as reliable and secure.

CT2. Customers trust the accuracy of our product information, prices, and transaction terms.

CT3. Customers believe that complaints and disputes will be handled fairly.

CT4. Customers perceive our online business as transparent and accountable.

E-Commerce Performance (EP)

- EP1. Our online sales performance has improved.
- EP2. Our customer retention and repeat purchasing have improved.
- EP3. Our online reputation and customer confidence have improved.
- EP4. Our e-commerce operations have become more stable and continuous.
- EP5. Our digital market growth and competitive position have improved.