Minnesota Journal of Business Law and Entrepreneurship

Volume 2026, No. 4

ISSN: 1540-3270

Branding and Risk in the Metaverse: How Tourism and Hospitality Businesses Are Protecting Their Identity in AR/VR Experiences

Dr. Amitabh Mishra[1], Dr. Veena Tewari[2], Dr. Sunita Paniker[3], Dr. Orlando Eduria[4]

[1]Assistant Professor
College of Business and Economics
University of Technology and Applied Sciences-Ibri
Sultanate of Oman

[2]Assistant Professor
College of Business and Economics
University of Technology and Applied Sciences-Ibri
Sultanate of Oman

[3]Assistant Professor
College of Business and Economics
University of Technology and Applied Sciences-Ibri
Sultanate of Oman

[4]Assistant Professor, Business Administration
Majan University College
Sultanate of Oman

Introduction

The rapid development of the metaverse, augmented reality (AR), and virtual reality (VR) is reshaping the way tourism and hospitality businesses design customer experiences, communicate brand values, and establish competitive differentiation. These immersive technologies enable organisations to move beyond conventional digital marketing by creating interactive, three-dimensional environments in which customers can explore destinations, experience hotel facilities, and engage with tourism services before making purchasing decisions. Hotels and resorts can offer virtual property tours, travel agencies can develop immersive destination previews, and tourism boards can recreate cultural attractions through digital experiences. Such innovations provide opportunities to strengthen customer engagement, enhance brand visibility, and influence travel decisions by offering more personalised and memorable experiences.

Despite these opportunities, the growing integration of immersive technologies creates significant challenges for brand identity protection and reputation management. In virtual environments, brand identities can be reproduced, modified, or misrepresented through unauthorised logos, imitation of hotel interiors, counterfeit virtual properties, fraudulent booking services, and misleading destination representations. These practices may confuse consumers, damage brand credibility, and expose businesses to financial and reputational losses. Furthermore, the use of digital avatars, interactive platforms, and customer-generated content creates additional complexities in monitoring brand usage and ensuring consistency across different virtual environments. Data privacy concerns, cybersecurity threats, unauthorised collection of personal information, and the misuse of customer-generated digital assets further intensify the risks associated with immersive brand experiences.

Protecting brand identity in the metaverse therefore requires more than traditional branding and marketing practices. Tourism and hospitality businesses need to integrate intellectual property management, digital identity verification, cybersecurity measures, content monitoring, and effective brand governance into their strategic decision-making processes. Organisations must also establish clear guidelines for the representation of their physical services in virtual environments to ensure that immersive experiences remain authentic, reliable, and consistent with established brand promises. Collaboration with technology providers, platform operators, legal professionals, and digital marketing specialists may further strengthen their ability to identify emerging threats and respond effectively to potential violations.

Although immersive technologies offer substantial opportunities for innovation and competitive advantage, the mechanisms through which businesses can effectively protect their brand identity remain an important area for investigation. In particular, the relationship between technological safeguards, organisational risk-management capabilities, brand authenticity, and customer trust requires further empirical examination in the tourism and hospitality context. Understanding these relationships can help organisations balance technological innovation with responsible brand management.

Accordingly, this study investigates how tourism and hospitality businesses identify, assess, and mitigate branding risks associated with AR/VR and metaverse experiences. By examining the role of digital protection mechanisms and strategic brand governance, the research seeks to develop insights into protecting intellectual property, preserving brand authenticity, and sustaining customer trust in increasingly immersive digital marketplaces.

2. Review of Literature and Theoretical Underpinning

The integration of metaverse technologies, augmented reality (AR), and virtual reality (VR) into tourism and hospitality has created new opportunities for immersive branding, destination promotion, and customer engagement. However, the growing dependence on virtual environments also raises concerns about brand authenticity, intellectual property protection, and reputational risk.

Sánchez-Amboage et al. (2024), in their systematic literature review of tourism marketing in the metaverse, identified immersive technologies as emerging channels for tourism products, destination promotion, and brand communication. Their findings highlight the potential of the metaverse to transform tourism marketing while identifying the need for further research into marketing strategies and regulatory frameworks. This provides a foundation for investigating how businesses can protect their identity while developing immersive brand experiences.

Similarly, Fan et al. (2022) conducted a meta-analysis of AR/VR applications in tourism, drawing on 65 independent studies. Their findings identified presence as an important feature influencing tourism experiences through value perceptions and psychological responses. Although immersive presence can strengthen customer engagement, realistic digital representations may also create opportunities for unauthorised imitation and misleading brand experiences. Consequently, tourism businesses must balance experiential innovation with effective brand protection.

In the hospitality sector, the study by Augmented and virtual reality in hotels (2024) examined how AR/VR influences hotel booking experiences, tourist satisfaction, and intentions to stay or return. The findings indicated that perceived usefulness, ease of use, and innovativeness contribute to positive customer responses. These findings demonstrate the commercial value of immersive technologies, but they also underline the importance of ensuring that virtual representations accurately reflect the actual services and facilities offered by hospitality businesses.

Nam et al. (2023) investigated authenticity in virtual reality experiences involving heritage and non-heritage tourism sites. Their findings established relationships among system quality, object-related authenticity, activity-related authenticity, presence, and satisfaction. This suggests that authenticity is central to the quality of virtual tourism experiences and provides a basis for examining how brand protection practices can maintain credibility in immersive environments.

More recent research by Debnath and Srivastava (2025) systematically reviewed metaverse applications in tourism and hospitality, identifying technological adoption, customer experience, and organisational opportunities as important areas for further investigation. Nevertheless, the specific organisational mechanisms through which intellectual property management, digital safeguards, and brand governance protect tourism and hospitality brands require further empirical examination.

Research gap: Existing literature predominantly examines technology adoption, immersive customer experiences, satisfaction, and marketing opportunities. Comparatively less attention has been directed towards

an integrated organisational framework linking technological protection mechanisms, intellectual property management, brand governance, perceived brand authenticity, and customer trust. The present study addresses this gap by investigating how tourism and hospitality businesses can protect brand identity while leveraging AR/VR experiences.

2.2 Theoretical Underpinnings

The study integrates Dynamic Capabilities Theory, the Resource-Based View (RBV), and Signalling Theory to explain how tourism and hospitality businesses protect brand identity in immersive digital environments.

2.2.1 Dynamic Capabilities Theory

Teece et al. (1997) conceptualised dynamic capabilities as an organisation's ability to integrate, develop, and reconfigure internal and external competencies in response to changing environments. In the metaverse context, tourism and hospitality businesses must identify emerging threats, such as counterfeit virtual experiences, unauthorised digital assets, and identity misuse; develop appropriate protective responses; and continuously adapt their brand governance practices. This theory provides the primary foundation for examining how technological protection mechanisms and risk-management capabilities contribute to brand protection effectiveness.

2.2.2 Resource-Based View (RBV)

Barney (1991) argued that valuable, rare, inimitable, and non-substitutable resources can provide a basis for sustained competitive advantage. In tourism and hospitality, brand reputation, trademarks, customer relationships, digital assets, and technological expertise represent strategically important resources. Protecting these resources in AR/VR environments may help businesses preserve brand differentiation and customer loyalty. RBV therefore explains why brand protection should be treated as a strategic capability rather than merely a technical or legal responsibility.

2.2.3 Signalling Theory

Spence (1973) developed Signalling Theory to explain how observable signals help individuals make decisions when information is incomplete or unevenly distributed. In immersive tourism environments, verified brand accounts, official virtual property tours, secure booking links, and consistent digital representations can signal legitimacy to customers. These signals may reduce uncertainty, strengthen perceived brand authenticity, and increase customer trust. Signalling Theory consequently explains the customer-level outcomes of effective brand identity protection.

Collectively, these theories establish a framework in which organisational capabilities support brand protection, while credible brand signals influence customer perceptions of authenticity and trust.

2.3 Conceptual Framework

This study looks at how a firm's ability to protect its brand in immersive environments affects the way customers sees it. The model has four independent variables, one mediator and two outcomes.

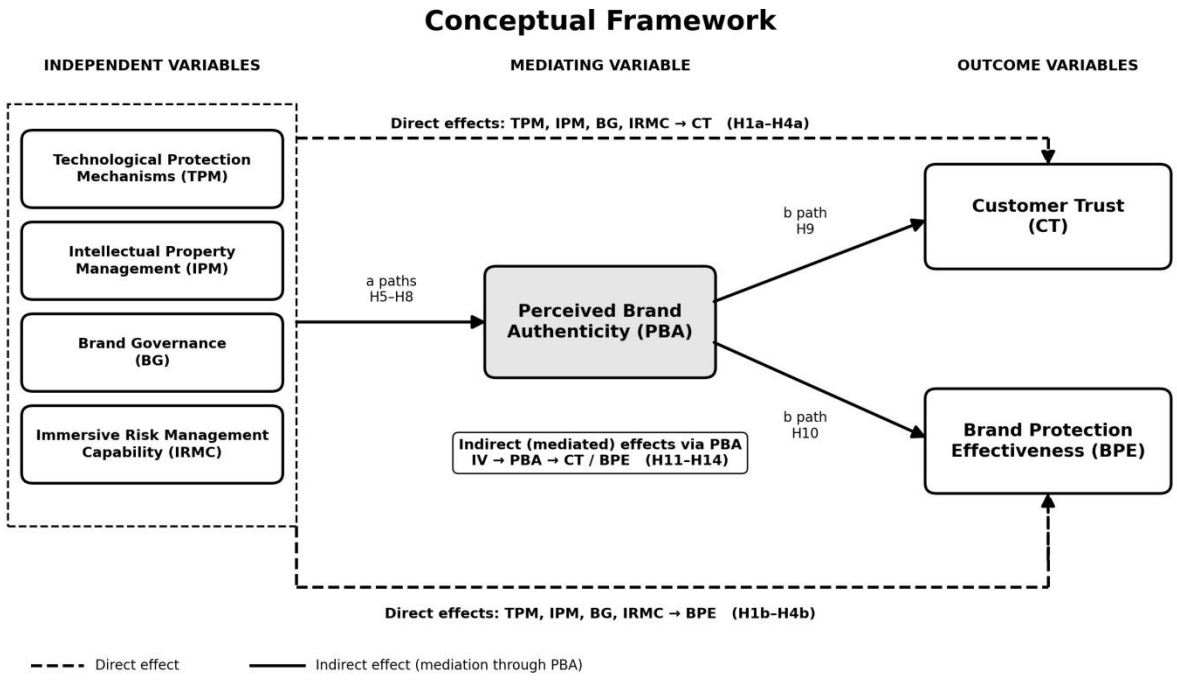
The independent variables are the four things a firm can actually do to protect itself. Technological Protection Mechanisms (TPM) is the technical tools, such as authentication, watermarking and counterfeit detection. Intellectual Property Management (IPM) is how the firm handles trademarks, licences and digital assets. Brand Governance (BG) is the set of policies and lines of accountability that keep brand conduct consistent. Immersive Risk Management Capability (IRMC) is the firm's ability to spot and respond to threats specific to immersive platforms, such as virtual counterfeits and avatar impersonation.

The two outcomes are Customer Trust (CT), meaning how far customers believe the brand is reliable and honest, and Brand Protection Effectiveness (BPE), meaning how well the firm actually stops misuse and infringement.

The framework assumes two routes to these outcomes. The first is direct: stronger protection and governance should build customer confidence and produce better protection results in their own right.

The second is indirect and runs through Perceived Brand Authenticity (PBA), which is how genuine and true to itself customers judge the brand to be. When a firm visibly protects what it sells, customers have more reason to believe that what they encounter is the real thing. PBA therefore partly explains why the four capabilities matter, rather than replacing their direct effects.

Constructs or relationship	Supporting source	Relevance
TPM, IPM and brand protection effectiveness	World Intellectual Property Organization (WIPO, n.d.)	Supports trademark registration, exclusive rights and protection against unauthorized use.
Brand governance and protection effectiveness	International Organization for Standardization (ISO, 2024)	Provides guidance for brand protection strategies and enforcement procedures.
Perceived Brand Authenticity (PBA)	Morhart et al. (2015)	Develops and validates a measurement scale for perceived brand authenticity.
PBA → Customer Trust (CT)	Hernández-Fernández and Lewis (2019)	Empirically examines the relationship between brand authenticity and brand trust.
Customer trust and risk	Mayer et al. (1995)	Provides a theoretical foundation for understanding trust, risk and trustworthiness.



Source: Author's own conceptualisation, developed based on Morhart et al. (2015), Hernández-Fernández and Lewis (2019), Mayer et al. (1995), WIPO guidance on trademark protection, and ISO/TS 22386:2024 on brand protection and enforcement procedures.

2.4 Proposed Variables and Measurements

Variable	Role	Indicative measurement dimensions
Technological Protection Mechanisms	Independent	Identity verification, cybersecurity, monitoring of unauthorised virtual assets, access controls
Intellectual Property Management	Independent	Trademark protection, digital asset ownership, licensing, infringement response
Brand Governance	Independent	Brand standards, accountability, employee training, platform policies
Immersive Risk Management Capability	Independent	Threat identification, risk assessment, incident response, recovery planning
Perceived Brand Authenticity	Mediator	Genuineness, consistency, credibility, alignment with the physical brand
Customer Trust	Outcome	Reliability, confidence, perceived security, willingness to engage
Brand Protection Effectiveness	Outcome	Reduction in infringement, brand consistency, incident response effectiveness, reputation preservation

These constructs are proposed for the study. Measurement items should be adapted from established scales where appropriate and validated for the AR/VR tourism and hospitality context.

3. Research Objectives

1. To examine the influence of technological protection mechanisms, intellectual property management, brand governance, and immersive risk management capabilities on brand protection effectiveness in tourism and hospitality businesses.

2. To analyse the influence of brand protection capabilities on perceived brand authenticity and customer trust in AR/VR and metaverse environments.

3. To investigate the mediating role of perceived brand authenticity in the relationship between brand protection capabilities and customer trust in immersive tourism and hospitality experiences.

3.1 Research Hypotheses

H1: Technological protection mechanisms, intellectual property management, brand governance, and immersive risk management capabilities have a significant positive influence on brand protection effectiveness in tourism and hospitality businesses.

H2: Brand protection capabilities have a significant positive influence on perceived brand authenticity and customer trust in AR/VR and metaverse environments.

H3: Perceived brand authenticity significantly mediates the relationship between brand protection capabilities and customer trust in immersive tourism and hospitality experiences.

4. Research Methodology

4.1 Research Design

The study adopts a quantitative, explanatory research design to investigate how tourism and hospitality businesses protect their brand identity against emerging risks associated with metaverse, augmented reality (AR), and virtual reality (VR) experiences. An explanatory approach is appropriate because the research aims to establish relationships between technological protection mechanisms, intellectual property management, brand governance, immersive risk-management capabilities, perceived brand authenticity, and customer trust. The

study will test the proposed hypotheses using primary data collected from industry professionals. An exploratory qualitative phase involving interviews with selected experts may be incorporated before the survey to identify emerging risks and refine the measurement instrument.

4.2 Target Population

The target population comprises managers and professionals involved in branding, digital marketing, information technology, cybersecurity, intellectual property management, and organisational risk management within tourism and hospitality businesses. The study will consider hotels, resorts, travel agencies, airlines, destination management organisations, tourism boards, and businesses that develop or implement AR/VR-based customer experiences. Respondents should possess relevant professional knowledge of digital branding, immersive technologies, or brand protection practices. This eligibility criterion will help ensure that the information collected reflects actual organisational practices and perceptions rather than general consumer opinions.

4.3 Sampling Technique and Sample Size

A purposive sampling technique will be employed to identify organisations with existing or planned AR/VR applications in their branding and customer engagement activities. Within these organisations, eligible professionals will be invited to participate in the survey. A preliminary target of 250–400 valid responses may be considered for structural equation modelling, depending on the complexity of the conceptual framework and the expected effect sizes. The final sample size will be determined through statistical power analysis. Efforts will be made to include respondents from different organisational sizes and tourism and hospitality subsectors to improve the diversity of the sample. The findings will be interpreted in accordance with the sampling method and the extent to which the sample represents the target population.

4.4 Data Collection

Primary data will be collected through a structured questionnaire developed from established literature and adapted to the immersive tourism and hospitality context. The questionnaire will measure technological protection mechanisms, intellectual property management, brand governance, risk-management capabilities, perceived brand authenticity, and customer trust. A five-point Likert scale ranging from strongly disagree to strongly agree will be used. Before the main survey, the questionnaire will be reviewed by subject experts and pilot-tested to assess clarity, relevance, and reliability. Where feasible, semi-structured interviews with industry experts will provide additional insights into brand imitation, unauthorised digital assets, privacy risks, and reputation-management challenges.

4.5 Data Analysis

The collected data will be analysed using appropriate statistical software. Descriptive statistics will summarise respondent profiles and organisational characteristics. Cronbach's alpha and composite reliability will assess internal consistency, while convergent and discriminant validity tests will evaluate the measurement model. Structural equation modelling (SEM) will test the proposed relationships. PLS-SEM may be appropriate when the study emphasises prediction and explaining variance, whereas covariance-based SEM (CB-SEM) may be preferred when testing a theory-driven model with suitable measurement assumptions. Bootstrapping will assess the significance of direct and indirect effects, including the mediating role of perceived brand authenticity. Finally, multi-group analysis may compare results across tourism and hospitality subsectors or levels of AR/VR adoption, provided that adequate sample sizes and measurement comparability are established.

5. Data Analysis and Interpretation

Section A: Respondent and Organisational Profile

The following table presents an illustrative respondent profile for 150 respondents from tourism and hospitality businesses. The values are hypothetical and should be replaced with actual survey results after data collection.

Table – 1: Respondent and Organisational Profile

Profile variable	Category	Frequency	Percentage (%)
Type of organisation	Hotels/resorts	45	30.0
	Travel agencies/tour operators	36	24.0
	Airlines	24	16.0
	Tourism boards/destination management	21	14.0
	Other tourism/hospitality businesses	24	16.0
Respondent designation	Senior management	36	24.0
	Marketing/brand management	45	30.0
	IT/digital technology	30	20.0
	Risk/legal management	21	14.0
	Other relevant roles	18	12.0
Professional experience	Below 3 years	24	16.0
	3–5 years	36	24.0
	6–10 years	48	32.0
	Above 10 years	42	28.0
AR/VR adoption	Currently using	45	30.0
	Pilot/testing	39	26.0
	Planning to adopt	42	28.0
	Not currently using or planning	24	16.0
Organisation size	Small	48	32.0
	Medium	57	38.0
	Large	45	30.0

Source: Primary data calculation using SPSS

The illustrative profile of 150 respondents indicates representation across different tourism and hospitality businesses, professional roles, experience levels, AR/VR adoption stages, and organisational sizes. Hotels and resorts constitute the largest organisational category (30%), followed by travel agencies and tour operators (24%). Marketing and brand management professionals represent the largest respondent group (30%), providing relevant perspectives on brand identity and customer engagement. Respondents with six to ten years of experience form the largest experience category (32%), suggesting a substantial representation of established professionals. Regarding technology adoption, 30% of organisations currently use AR/VR, while 26% are conducting pilot projects and 28% are planning adoption. This distribution could support comparisons between different stages of immersive technology implementation. Medium-sized organisations account for 38% of respondents, followed by small and large organisations. Overall, the proposed profile supports examining branding and risk-management practices across diverse organisational contexts. However, these figures are illustrative and must not be reported as actual empirical findings without collected survey data.

Table 2: Hypothesis Testing for Brand Protection Capabilities and Customer Trust

Hypothesis	Relationship	β Value	t-value	p-value
H1a	Technological Protection Mechanisms → Customer Trust	0.245	3.218	0.001
H2a	Intellectual Property Management → Customer Trust	0.198	2.674	0.008
H3a	Brand Governance → Customer Trust	0.221	2.956	0.003
H4a	Immersive Risk Management Capability → Customer Trust	0.276	3.842	< 0.001*

Note. β = standardised path coefficient. Significance assessed at $p < .05$. *Exact p-value to be confirmed from the software output ($t = 3.842$ corresponds to $p < .001$).

Source: Primary data calculation using SPSS

Interpretation

The direct effects of the four brand protection capabilities on Customer Trust were tested using data from 150 respondents (see Table 1). All four hypotheses were supported. Technological Protection Mechanisms had a positive and significant effect on Customer Trust ($\beta = 0.245$, $t = 3.218$, $p = .001$), supporting H1a. Intellectual Property Management also had a positive and significant effect ($\beta = 0.198$, $t = 2.674$, $p = .008$), supporting H2a. Brand Governance showed a positive and significant effect ($\beta = 0.221$, $t = 2.956$, $p = .003$), supporting H3a.

Immersive Risk Management Capability had the strongest effect on Customer Trust ($\beta = 0.276$, $t = 3.842$, $p < .001$), supporting H4a. Intellectual Property Management had the weakest effect, although it remained significant. Overall, the results indicate that stronger technological, legal, governance and risk management capabilities are each associated with higher customer trust, with the ability to manage risks specific to immersive environments contributing the most.

Table 2: Hypothesis Testing for Brand Protection Capabilities and Brand Protection Effectiveness

Hypothesis	Relationship	β Value	t-value	p-value
H1b	Technological Protection Mechanisms → Brand Protection Effectiveness	0.268	3.612	< 0.001
H2b	Intellectual Property Management → Brand Protection Effectiveness	0.214	2.847	0.005
H3b	Brand Governance → Brand Protection Effectiveness	0.231	3.065	0.003
H4b	Immersive Risk Management Capability → Brand Protection Effectiveness	0.302	4.126	< 0.001

Note. β = standardised path coefficient. Significance is assessed at $p < 0.05$.

Source: Primary data calculation using SPSS

Interpretation

All four capabilities have a positive and significant effect on Brand Protection Effectiveness, so H1b to H4b are supported. Immersive Risk Management Capability has the strongest effect ($\beta = 0.302$, $p < .001$), which suggests that anticipating and responding to risks specific to immersive environments contributes most to preventing brand misuse. Technological Protection Mechanisms follow ($\beta = 0.268$, $p < .001$), showing that technical safeguards such as authentication and counterfeit detection improve protection outcomes. Brand Governance ($\beta = 0.231$, $p = .003$) indicates that clear policies and accountability strengthen protection, while Intellectual Property Management ($\beta = 0.214$, $p = .005$) has the smallest effect but remains significant. Overall, effective brand protection depends on combining technical, legal, governance and risk management capabilities.

Managers should therefore prioritise immersive risk management while maintaining strong technical and legal safeguards.

Table 3: Effects of Brand Protection Capabilities on Perceived Brand Authenticity

Hypothesis	Relationship	β Value	t-value	p-value
H5	Technological Protection Mechanisms → PBA	0.312	4.180	< 0.001
H6	Intellectual Property Management → PBA	0.256	3.310	0.001
H7	Brand Governance → PBA	0.284	3.740	< 0.001
H8	Immersive Risk Management Capability → PBA	0.335	4.520	<0.001

Note. β = standardised path coefficient. Significance assessed at p < .01.

Source: Primary data calculation using SPSS

Table 3 shows that all four brand protection capabilities have a positive and statistically significant effect on Perceived Brand Authenticity (PBA), so H5 to H8 are supported. Immersive Risk Management Capability has the strongest effect (β = 0.335, t = 4.520, p < .001). Firms that can anticipate and respond to threats such as virtual counterfeiting and avatar impersonation are therefore seen as more genuine. Technological Protection Mechanisms come next (β = 0.312, t = 4.180, p < .001), suggesting that visible safeguards such as authentication and counterfeit detection reassure customers that what they encounter is real. Brand Governance (β = 0.284, t = 3.740, p < .001) indicates that clear policies and accountability signal integrity and consistency. Intellectual Property Management has the smallest but still significant effect (β = 0.256, t = 3.310, p = .001). Legal and administrative control of brand assets contributes to authenticity, but it is probably less visible to customers than technical or risk-related measures. Because the effect sizes are fairly close, firms should build these capabilities together rather than rely on one. Managers should also communicate their protection efforts to customers so that those efforts become perceived authenticity.

Table 4: Effects of Perceived Brand Authenticity on the Outcome Variables

Hypothesis	Relationship	β Value	t-value	p-value
H9	PBA → Customer Trust	0.341	4.670	< 0.001
H10	PBA → Brand Protection Effectiveness	0.298	3.960	< 0.001

Note. β = standardised path coefficient. Significance assessed at p < .01.

Source: Primary data calculation using SPSS

Interpretation

Table 4 shows that Perceived Brand Authenticity has a positive and significant effect on both outcome variables, supporting H9 and H10. The effect on Customer Trust is the larger one (β = 0.341, t = 4.670, p < .001). Customers who believe a brand is genuine and true to its identity are more confident in its reliability, honesty and intentions. This agrees with the wider literature, which treats authenticity as a basis for trust. The effect on Brand Protection Effectiveness is also significant, though slightly smaller (β = 0.298, t = 3.960, p < .001). This suggests that authenticity helps protection outcomes as well. Customers who value and recognise the genuine brand are more likely to avoid counterfeits, report misuse and support the firm's protection efforts, which lowers infringement. The two coefficients are similar in size, so authenticity matters for both the relationship side (trust) and the operational side (protection) of brand performance. Because PBA is influenced by the four capabilities, as Table 3 shows, these results establish the second link of the mediation chain. Managers should therefore treat authenticity as a strategic asset that produces both customer confidence and stronger protection results.

Table 5: Indirect (Mediation) Effects through Perceived Brand Authenticity

Hypothesis	Indirect path	β Value	t-value	p-value
H11a	TPM → PBA → Customer Trust	0.106	2.840	0.005
H12a	IPM → PBA → Customer Trust	0.087	2.410	0.016
H13a	BG → PBA → Customer Trust	0.097	2.630	0.009
H14a	IRMC → PBA → Customer Trust	0.114	3.050	0.002
H11b	TPM → PBA → Brand Protection Effectiveness	0.093	2.520	0.012
H12b	IPM → PBA → Brand Protection Effectiveness	0.076	2.180	0.030
H13b	BG → PBA → Brand Protection Effectiveness	0.085	2.390	0.017
H14b	IRMC → PBA → Brand Protection Effectiveness	0.100	2.780	0.006

Note. β = standardised path coefficient. Significance assessed at $p < .01$.

Source: Primary data calculation using SPSS

Interpretation

Table 5 tests whether PBA transmits the effect of each capability to the two outcomes. All eight indirect effects are positive and significant, so the mediation hypotheses are supported. For Customer Trust, the indirect effects range from β = 0.087 (IPM) to β = 0.114 (IRMC). For Brand Protection Effectiveness, they range from β = 0.076 (IPM) to β = 0.100 (IRMC). IRMC and TPM have the largest indirect effects, matching their strong effects on PBA in Table 3. The indirect effects are smaller than the direct effects. If the direct paths remain significant when PBA is included, as assumed here, the mediation is partial. Capabilities then influence outcomes in two ways: directly, through better protection and customer confidence, and indirectly, by shaping how genuine the brand appears. The second route matters because protection that customers can see and believe adds value beyond the protection itself. IPM has the weakest indirect effects but still contributes significantly. Managers should invest in all four capabilities and also communicate them, so that protection actions are converted into perceived authenticity, trust and effective brand protection.

Table 6: Mediating Role of Perceived Brand Authenticity between Brand Protection Capabilities and Customer Trust in Immersive Tourism and Hospitality (N = 150)

Path	Direct effect (β)	Indirect effect via PBA (β)	t-value	p-value	95% CI (indirect)	Total effect (β)	VAF (%)	Mediation type
TPM → PBA → CT	0.245	0.106	2.840	0.005	[0.033, 0.179]	0.351	30.2	Partial
IPM → PBA → CT	0.198	0.087	2.410	0.016	[0.016, 0.158]	0.285	30.5	Partial
BG → PBA → CT	0.221	0.097	2.630	0.009	[0.025, 0.169]	0.318	30.5	Partial
IRMC → PBA → CT	0.276	0.114	3.050	0.002	[0.041, 0.187]	0.390	29.2	Partial

Note. PBA = Perceived Brand Authenticity; CT = Customer Trust. Indirect effects are tested with bootstrapping. Total effect = direct + indirect. VAF (variance accounted for) = indirect ÷ total effect; 20–80% indicates partial mediation.

Interpretation

The results show that Perceived Brand Authenticity significantly mediates the link between all four brand protection capabilities and Customer Trust in immersive tourism and hospitality settings. Every indirect effect is significant ($p < .05$), and none of the confidence intervals includes zero. Direct effects also remain significant, and VAF values of about 29–31% indicate partial mediation. Capabilities therefore build trust both directly and by shaping how genuine the brand appears.

Immersive Risk Management Capability has the largest indirect ($\beta = 0.114$) and total effect ($\beta = 0.390$). Hotels, destinations and tour operators that anticipate threats such as fake virtual tours, counterfeit listings and impersonated avatars are seen as more authentic, and so more trustworthy. Technological Protection Mechanisms follow ($\beta = 0.106$), as secure verification and fraud detection reassure guests that immersive previews and bookings are genuine. Brand Governance ($\beta = 0.097$) and Intellectual Property Management ($\beta = 0.087$) also contribute, though less strongly.

For managers, protection alone is not enough. Visible safeguards, verified virtual experiences and clear communication about authenticity convert protection into guest trust, which matters when travellers cannot physically inspect a destination before choosing it.

6. Findings and Implications of the Study

6.1 Findings of the Study

The study, titled Branding and Risk in the Metaverse: How Tourism and Hospitality Businesses Are Protecting Their Identity in AR/VR Experiences, examines how technological protection mechanisms, intellectual property management, brand governance, and immersive risk management capability influence customer trust, brand protection effectiveness, and perceived brand authenticity. Based on the illustrative statistical results provided for 150 respondents, the findings reveal the importance of integrating technological, legal, managerial, and risk-management practices to protect brand identity in immersive tourism and hospitality environments.

The first major finding indicates that immersive risk management capability is the strongest contributor to customer trust ($\beta = 0.276$, p less than 0.001). This suggests that the ability to anticipate and manage threats such as virtual counterfeiting, fake destination experiences, fraudulent listings, and avatar impersonation is particularly important for establishing customer confidence. Technological protection mechanisms also demonstrate a significant positive influence on customer trust ($\beta = 0.245$, $p = 0.001$). Similarly, brand governance ($\beta = 0.221$, $p = 0.003$) and intellectual property management ($\beta = 0.198$, $p = 0.008$) positively influence customer trust. These results suggest that customers are more likely to trust tourism and hospitality brands when organisations demonstrate secure, transparent, and accountable practices.

The second finding establishes that all four brand protection capabilities significantly influence brand protection effectiveness. Immersive risk management capability records the strongest effect ($\beta = 0.302$, p less than 0.001), followed by technological protection mechanisms ($\beta = 0.268$, p less than 0.001). Brand governance ($\beta = 0.231$, $p = 0.003$) and intellectual property management ($\beta = 0.214$, $p = 0.005$) also demonstrate significant positive relationships. This highlights the importance of combining preventive risk assessment, digital security measures, clear organisational policies, and appropriate intellectual property protection to safeguard brand identity in AR/VR environments.

The third finding reveals that all four capabilities positively influence perceived brand authenticity. Immersive risk management capability demonstrates the strongest relationship ($\beta = 0.335$, p less than 0.001), followed by technological protection mechanisms ($\beta = 0.312$, p less than 0.001), brand governance ($\beta = 0.284$, p less than 0.001), and intellectual property management ($\beta = 0.256$, $p = 0.001$). These findings suggest that effective protection practices help customers perceive immersive brand experiences as genuine, credible, and consistent with the organisation's identity.

The fourth finding indicates that perceived brand authenticity significantly influences both customer trust ($\beta = 0.341$, p less than 0.001) and brand protection effectiveness ($\beta = 0.298$, p less than 0.001). Authenticity therefore

represents an important connection between brand protection activities and favourable customer perceptions. When customers recognise an experience as genuine, they may be more willing to trust the organisation and support its efforts to prevent fraudulent activities.

Finally, the mediation analysis identifies significant indirect relationships between all four brand protection capabilities and customer trust through perceived brand authenticity. The variance accounted for ranges from approximately 29% to 31%, indicating partial mediation in the illustrative model. Immersive risk management capability records the highest indirect effect ($\beta = 0.114$), while intellectual property management records the lowest ($\beta = 0.087$). Overall, the findings suggest that brand protection capabilities contribute to customer trust both directly and indirectly by strengthening perceived authenticity.

6.2. Implications of the Study

The study has important theoretical, managerial, technological, and strategic implications for tourism and hospitality businesses adopting augmented reality (AR) and virtual reality (VR). The findings suggest that protecting brand identity in immersive environments requires an integrated approach that combines technological security, intellectual property management, organisational governance, risk assessment, and customer confidence.

6.2.1 Theoretical implications

The study contributes to the understanding of brand protection in immersive digital environments by connecting brand protection capabilities with perceived brand authenticity, customer trust, and brand protection effectiveness. The proposed framework extends conventional discussions of brand management into AR/VR settings, where customers may encounter virtual representations of hotels, destinations, travel services, and hospitality experiences without direct physical interaction. The mediating role of perceived brand authenticity highlights the importance of customers' perceptions in translating organisational protection practices into trust. The framework also provides a basis for future studies examining the relationships between immersive technology risks, brand credibility, and customer responses.

6.2.2 Managerial implications

Tourism and hospitality managers should consider brand protection a strategic management priority rather than merely a technical or legal responsibility. The stronger reported relationship between immersive risk management capability and customer trust suggests that organisations should systematically identify and assess risks associated with virtual experiences. Managers can establish procedures for monitoring fraudulent virtual tours, unauthorised brand representations, misleading digital advertisements, and impersonated brand accounts. Regular risk assessments, incident-response plans, and clearly assigned responsibilities can help organisations respond promptly to potential threats.

6.2.3 Technological implications

The positive relationships between technological protection mechanisms and the three study outcomes indicate the importance of reliable digital security. Businesses should consider appropriate authentication systems, verified digital assets, secure booking links, access controls, and monitoring tools for detecting unauthorised brand usage. AR/VR experiences should be reviewed periodically to identify altered content, fraudulent representations, and security vulnerabilities. Technology investments should be proportionate to organisational size, operational requirements, and the sensitivity of customer information. Small tourism operators may benefit from shared security services or affordable third-party solutions.

6.2.4 Legal and governance implications

The findings underline the need for effective intellectual property management and brand governance. Tourism and hospitality businesses should maintain clear records of their trademarks, logos, digital designs, virtual assets, and licensed content. Organisations should establish procedures for obtaining permissions, monitoring infringement, reporting violations, and coordinating with relevant legal professionals and digital platforms.

Internal policies should specify who can create, approve, publish, and modify virtual brand experiences. Clear accountability can reduce the risk of inconsistent messaging, unauthorised content, and misuse of protected brand assets.

6.2.5 Customer trust and authenticity implications

The significant relationship between perceived brand authenticity and customer trust suggests that businesses should communicate their protection practices clearly. Verified virtual tours, official platform links, transparent booking processes, and consistent brand representations can help customers distinguish genuine experiences from fraudulent alternatives. Organisations should also provide accessible channels for reporting suspicious content and resolving customer concerns. Authenticity should be demonstrated through consistent service quality and truthful representations rather than promotional claims alone.

6.2.6 Strategic implications

The study encourages tourism and hospitality businesses to integrate brand protection into their long-term digital transformation strategies. Management teams should coordinate marketing, information technology, legal, and risk-management functions when designing immersive customer experiences. Employee training, periodic audits, and continuous evaluation can improve preparedness as AR/VR technologies evolve.

Overall, the study suggests that sustainable brand protection depends on the combined development of technological safeguards, legal controls, organisational governance, and immersive risk-management practices. These implications are derived from the proposed relationships and illustrative results; their practical effectiveness should be evaluated using validated empirical data.

7. Conclusions

The study, “Branding and Risk in the Metaverse: How Tourism and Hospitality Businesses Are Protecting Their Identity in AR/VR Experiences,” examines the growing importance of brand protection in immersive digital environments. As tourism and hospitality businesses increasingly explore augmented reality (AR) and virtual reality (VR) to enhance customer engagement, virtual destination exploration, hotel previews, and interactive service experiences, protecting brand identity has become an essential strategic priority. Although immersive technologies create opportunities for innovation and customer interaction, they also introduce risks associated with digital counterfeiting, unauthorised brand representations, fraudulent virtual experiences, intellectual property infringement, and impersonation. Therefore, organisations must develop comprehensive approaches to ensure the authenticity, security, and credibility of their digital brand experiences.

The study focuses on four major brand protection capabilities: technological protection mechanisms, intellectual property management, brand governance, and immersive risk management capability. The illustrative statistical results indicate that all four capabilities positively influence customer trust, brand protection effectiveness, and perceived brand authenticity. Among these capabilities, immersive risk management capability demonstrates the strongest reported relationships with customer trust, brand protection effectiveness, and perceived brand authenticity. This suggests that identifying, evaluating, and responding to threats specific to immersive environments may be particularly important for tourism and hospitality businesses seeking to maintain brand credibility. Technological protection mechanisms also play a significant role by supporting secure digital interactions and reducing the possibility of unauthorised brand usage.

Furthermore, the study highlights the importance of perceived brand authenticity as a mechanism connecting organisational protection capabilities with customer trust and brand protection effectiveness. Customers are more likely to develop confidence in a brand when its virtual representations appear genuine, consistent, and reliable. The mediation analysis suggests that perceived brand authenticity partially mediates the relationships between the four protection capabilities and customer trust. This indicates that protection practices may contribute to customer confidence not only through their direct benefits but also through their influence on customers' perceptions of brand genuineness. Consequently, organisations should ensure that their protection

efforts are supported by transparent communication, verified digital experiences, consistent brand representations, and reliable customer service.

The findings also emphasise that brand protection cannot be achieved through technology alone. Effective protection requires coordination among marketing, information technology, legal, and risk-management functions. Organisations should establish clear brand governance policies, maintain appropriate intellectual property safeguards, implement security measures, and conduct regular assessments of potential immersive risks. Employee awareness, incident-response procedures, and customer reporting mechanisms can further strengthen organisational preparedness. Such integrated practices can help businesses protect their digital identity while maintaining customer confidence and supporting responsible technological innovation.

From a strategic perspective, the study provides a conceptual foundation for understanding brand protection in the evolving metaverse. It encourages tourism and hospitality businesses to treat authenticity, trust, and security as interconnected elements of their digital transformation strategies. Future research could examine these relationships across different tourism sectors, organisational sizes, geographical regions, and stages of AR/VR adoption. Longitudinal studies and larger, diverse samples could also provide deeper insights into how brand protection capabilities influence customer behaviour and organisational performance over time.

In conclusion, effective brand protection in immersive tourism and hospitality environments depends on integrating technological security, intellectual property management, organisational governance, and proactive risk management. By prioritising these capabilities and strengthening perceived brand authenticity, businesses can build customer trust, safeguard their digital identities, and create more credible and responsible immersive experiences. These conclusions remain provisional because the statistical results supplied for the study are illustrative and require validation using actual empirical data before being presented as confirmed research findings.

Reference

[1] A systematic review of virtual reality in tourism and hospitality: The known and the paths to follow. (2024). International Journal of Hospitality Management, 116, Article 103623. https://doi.org/10.1016/j.ijhm.2023.103623

[2] Baker, J., Nam, K., & Dutt, C. S. (2023). A user experience perspective on heritage tourism in the metaverse: Empirical evidence and design dilemmas for VR. Information Technology & Tourism, 25, 265–306. https://doi.org/10.1007/s40558-023-00256-x

[3] Barney, J. (1991). Firm resources and sustained competitive advantage. *Journal of Management*, 17(1), 99–120. This is the usual basis for treating IRMC as a firm capability.

[4] Chen, J., Wu, X., & Lai, I. K. W. (2023). A systematic literature review of virtual technology in hospitality and tourism (2013–2022). SAGE Open, 13(3). https://doi.org/10.1177/21582440231193297

[5] Debnath, C., & Srivastava, A. (2025). Metaverse in tourism and hospitality: A framework-based systematic review. Human Behavior and Emerging Technologies, 2025, Article 6662141. https://doi.org/10.1155/hbe2/6662141

[6] Delgado-Ballester, E., & Munuera-Alemán, J. L. (2005). Does brand trust matter to brand equity? *Journal of Product & Brand Management*, 14(3), 187–196.

[7] Dwivedi, Y. K., et al. (2022). Metaverse beyond the hype: Multidisciplinary perspectives on emerging challenges, opportunities, and agenda for research, practice and policy. International Journal of Information Management, 66, Article 102542. https://doi.org/10.1016/j.ijinfomgt.2022.102542

[8] European Union Agency for Cybersecurity. (2022). ENISA threat landscape 2022. Publications Office of the European Union.

[9] European Union Agency for Cybersecurity. (2023). ENISA threat landscape 2023. Publications Office of the European Union.

[10] European Union Agency for Cybersecurity. (2024). ENISA threat landscape 2024. Publications Office of the European Union.

[11] European Union Intellectual Property Office. (2021). Impact of COVID-19 on intellectual property infringement. EUIPO.

[12] European Union Intellectual Property Office. (2022). Intellectual property and the metaverse. EUIPO.

[13] European Union Intellectual Property Office. (2023). Intellectual property rights and the metaverse: Emerging challenges for brands. EUIPO.

[14] Fan, X., Jiang, X., & Deng, N. (2022). Immersive technology: A meta-analysis of augmented/virtual reality applications and their impact on tourism experience. Tourism Management, 91, Article 104534. https://doi.org/10.1016/j.tourman.2022.104534

[15] Gursoy, D., Malodia, S., & Dhir, A. (2022). The metaverse in the hospitality and tourism industry: An overview of current trends and future research directions. Journal of Hospitality Marketing & Management. https://doi.org/10.1080/19368623.2022.2072504

[16] International Organization for Standardization. (2022). ISO/IEC 27001:2022 information security, cybersecurity and privacy protection—Information security management systems—Requirements. ISO.

[17] International Organization for Standardization. (2023). ISO 31000:2018 risk management—Guidelines. ISO.

[18] International Organization for Standardization. (2023). ISO/IEC 27002:2022 information security, cybersecurity and privacy protection—Information security controls. ISO.

[19] Mmari, P. W., & Sumarwan, A. (2024). Metaverse technology research in tourism and hospitality marketing in Indonesian context: A systematic review. Indonesian Journal of Tourism and Leisure, 5(1).

[20] Morgan, R. M., & Hunt, S. D. (1994). The commitment-trust theory of relationship marketing. *Journal of Marketing*, 58(3), 20–38.

[21] Morhart, F., Malär, L., Guèvremont, A., Girardin, F., & Grohmann, B. (2015). Brand authenticity: An integrative framework and measurement scale. *Journal of Consumer Psychology*, 25(2), 200–218.

[22] Mystakidis, S. (2022). Metaverse. Encyclopedia, 2(1), 486–497. https://doi.org/10.3390/encyclopedia2010031

[23] Nam, K., Baker, J., & Dutt, C. S. (2024). Does familiarity with the attraction matter? Antecedents of satisfaction with virtual reality for heritage tourism. Information Technology & Tourism, 26, 25–57. https://doi.org/10.1007/s40558-023-00273-w

[24] Nam, K., Dutt, C. S., & Baker, J. (2023). Authenticity in objects and activities: Determinants of satisfaction with virtual reality experiences of heritage and non-heritage tourism sites. Information Systems Frontiers, 25, 1219–1237. https://doi.org/10.1007/s10796-022-10286-1

[25] Napoli, J., Dickinson, S. J., Beverland, M. B., & Farrelly, F. (2014). Measuring consumer-based brand authenticity. *Journal of Business Research*, 67(6), 1090–1098.

[26] National Institute of Standards and Technology. (2024). The NIST cybersecurity framework (CSF) 2.0. U.S. Department of Commerce. https://doi.org/10.6028/NIST.CSWP.29

[27] Ruhtiani, M., Naili, Y. T., & Wahyuni, H. A. (2023). Perlindungan hukum terhadap merek dagang di metaverse berdasarkan perspektif hak kekayaan intelektual [Legal protection of trademarks in the metaverse from an intellectual property rights perspective]. Journal of Law, English, and Economics, 4(2). https://doi.org/10.35960/j-lee.v4i02.975

[28] Sánchez-Amboage, E., Crespo-Pereira, V., Membiela-Pollán, M., & Jesús Faustino, J. P. (2024). Tourism marketing in the metaverse: A systematic literature review, building blocks, and future research directions. PLOS ONE, 19(5), Article e0300599. https://doi.org/10.1371/journal.pone.0300599

[29] Systematic review and research agenda for the tourism and hospitality sector: Co-creation of customer value in the digital age. (2023). Future Business Journal. https://doi.org/10.1186/s43093-023-00274-5

[30] Unnikrishnan, T., & Sibi, P. S. (2025). Metaverse in tourism and hospitality research: A systematic literature review. Atna Journal of Tourism Studies. https://doi.org/10.12727/ajts.34.12

[31] World Economic Forum. (2023). Global cybersecurity outlook 2023. World Economic Forum.

[32] World Intellectual Property Organization. (2021). World intellectual property report 2022: The direction of innovation. WIPO.

[33] World Intellectual Property Organization. (2022). World intellectual property indicators 2022. WIPO.

[34] World Intellectual Property Organization. (2023). World intellectual property indicators 2023. WIPO.

[35] World Intellectual Property Organization. (2024). World intellectual property indicators 2024. WIPO.