JOURNAL OF Emerging Paradigms in Computing Systems JEPCS

Journal of Emerging Paradigms in Computing Systems (JEPCS) | Volume 01, Issue No. 02, 2025

ARTICLE TYPE: Research Article

Article ID: JEPCS-2025-0102-0023

Governance of Generative AI in Bank Marketing Content in Pakistan: Copyright, Trade Mark Protection, Deepfake Impersonation, and Compliance by Design

Madiha Awais[1,*],

[1] Lahore Business School, The University of Lahore, Lahore, Pakistan

*Corresponding author: madiha.awais@lbs.uol.edu.pk

Contributing author: madiha.awais@lbs.uol.edu.pk

Received: April 14, 2025 **Accepted:** June 28, 2025

Abstract- Generative artificial intelligence (GenAI) can be used in bank marketing to prepare advertising copy, fake images, conversational content, and personalized offers. Its use in banking also creates problems that are not limited to marketing quality. Incorrect product information, unauthorized use of protected material, fake endorsements, or impersonated content can affect customers and expose banks to legal and regulatory concerns. In this paper, we propose a governance and compliance framework for the use of GenAI in bank marketing in Pakistan. The framework covers rights clearance for source material and generated content, review of product claims, disclosure and content provenance, privacy and fairness in personalized marketing, and response to deepfake-enabled impersonation and brand spoofing. We develop these controls with reference to Pakistan's laws and regulatory requirements concerning trademarks, copyright, deceptive marketing, consumer protection, customer data, and cybercrime. Relevant banking technology-governance requirements and international AI-governance principles are also considered. A scenario-based case study is used to explain how the controls apply during content preparation, review, publication, targeting, and post-publication monitoring. The framework also defines responsibilities and records that can be used for review and audit. Its effectiveness is not empirically evaluated in this study and remains a subject for future work.

Keywords- Generative AI; Banking Marketing; Copyright; Trade Marks; Deepfakes

1. Introduction

Banks in Pakistan communicate with customers through several digital channels, including mobile applications, digital banking platforms, social-media campaigns, personalized offers, chatbots, and other conversational interfaces. Customers utilize these messages to learn about financial products, fees, eligibility requirements, and available services, thus their reliability is crucial. It is now possible to create advertising copy, customer messaging, product descriptions, campaign images, and various forms of promotional content using GenAI, which includes massive language models and image-generation systems. An activity that already relies on precise information and unambiguous identification of the bank as the source of communication is made riskier by its usage. Another challenge is use of deceptive or protected content. A produced phrase, picture, logo, or campaign design can be similar to another brand or imply an unapproved affiliation. When copyrighted content is fed into a GenAI system or when the output replicates protected expression, copyright problems may also arise. Another issue is that deepfake movies, cloned sounds, and synthetic people might lead to customers accepting altered content as official bank correspondence. External actors can also utilize GenAI to replicate a bank's identity and spread phony promotional messages or ads. As a result, the issue is not exclusive to information produced by banks. It also covers the abuse of the bank's brand by using fake and fake material.

Parts of this issue have been addressed in earlier research. Duivenvoorde [1] examines GenAI-based marketing from the standpoint of consumer protection and talks about transparency, accountability, and enforcement. In [2], the authors investigate how consumers evaluate the legitimacy and authenticity of synthetic adverts in order to determine the impact of transparency in deepfake advertising. Concerns about copyright and other intellectual property have also been mentioned as obstacles to using GenAI in marketing [3]. These studies are helpful for comprehending specific concerns, but they don't explain how these risks might be managed collectively in Pakistan's financial and judicial systems.

The usage of GenAI in bank marketing within Pakistan's current institutional and regulatory framework is examined in this article. In addition to consumer protection and competition law concepts pertaining to deceptive advertising and unfair market practices [4], the study takes into account the Trade Marks Ordinance 2001 and the Copyright Ordinance 1962. Impersonation, fraudulent campaigns, and misuse of synthetic media are also taken into consideration under the Prevention of Electronic Crimes Amendment Act 2025 [5]. Based on these requirements, we propose a governance approach for GenAI-assisted bank marketing and relate it to the State Bank of Pakistan's technology-governance expectations and relevant international AI governance standards [6,7]. The study is limited to bank marketing and related content operations. The research question addressed in this paper is: how can banks in Pakistan use GenAI for marketing and content operations while maintaining legal accountability, protecting customers, preserving brand integrity, and safeguarding fundamental rights? The main contributions of this paper are given below:

- We identify the main legal and governance risks that arise when GenAI is used in bank marketing in Pakistan and relate these risks to the relevant legal obligations and enforcement considerations.
- We propose a compliance framework in which intellectual property, consumer protection, transparency, privacy, fairness, and deepfake response are handled within the bank marketing process.
- Two workflow figures are used to present the governance controls for GenAI-assisted marketing and the response process for deepfake-enabled bank impersonation.
- The practical implementation of the proposed restrictions is demonstrated through a case study of the banking industry. Additionally, the study identifies indicators that may be utilized for empirical evaluation and auditing in the future.

The remainder of the paper is organized as follows. In Section 2, related work on deepfake disclosure, consumer protection, GenAI marketing, intellectual property, and governance requirements is presented. The legal and regulatory environment of Pakistan is covered in Section 3. The study's scope and research design are described in Section 4. The suggested compliance structure is presented in Section 5, and the deepfake and impersonation response sequence is explained in Section 6. The case study of the banking industry and the suggested audit indicators are presented in Section 7. The results and restrictions are described in Section 8. The paper is concluded in Section 9.

2. Related Work

2.1. GenAI Marketing and Consumer Protection

Advertising copy, customized offers, customer messaging, and several campaign content versions may all be created using GenAI. When describing fees, product conditions, eligibility requirements, or transactions, the accuracy of such information is crucial in the banking industry. When comparing or choosing financial products, customers may utilize this information. The author examines GenAI-based marketing from the standpoint of consumer protection in [1]. In addition to highlighting issues with opacity, enforcement, and consumer vulnerability, the paper explores how current consumer protection laws may apply to generative advertising. These concerns are pertinent to bank marketing because, although appearing to be professionally written, produced material may be erroneous, ambiguous, or lacking.

2.2. Deepfakes, Disclosure, and Trust

Deepfake advertising presents a unique problem as the consumer needs to decide whether the communication is genuine before acting upon it. This problem is important for banks as promotional messages may be sent through the same channels as security alerts, product information, and other official mail. The authors of [2] investigate how consumers react to deepfake advertising and how perceptions of authenticity, purpose, and trust are impacted by disclosure. According to the study, transparency affects how individuals see deceptive advertising. Customers may find it challenging to choose between authentic content and content that has been altered or faked in banking due to inadequate or ambiguous information. As a result, disclosure by itself is insufficient and both the source and communication channel must also be taken into account.

2.3. Intellectual Property in Generative Systems

Further concerns raised by GenAI-assisted marketing include copyright, ownership, and the use of protected information. In [8], the author discusses ownership, training data, and the interests of rights holders in generative systems. These issues become relevant to banks when employees use third-party images, slogans, textual content, music, or brand elements as recommendations or source material. The generated output may also require review if it reproduces or closely resembles protected expression. Trademark-related concerns are discussed in [9]. The authors examine AI-driven content creation in relation to trademark misuse, counterfeiting, impersonation, and consumer confusion. For bank marketing, the risk can arise from the material entered into the GenAI system as well as from the generated output. Industry evidence also reports copyright and intellectual property concerns as barriers to the wider use of GenAI in marketing [3]. These studies support the need to review both source material and generated content before publication.

2.4. Governance Standards Relevant to Banks

Banks also require a governance structure for controlling how AI systems are selected, used, reviewed, and monitored. ISO/IEC 42001 provides an AI management-system approach based on organizational policy, lifecycle controls, risk assessment, monitoring, and continual improvement [10]. The NIST AI Risk Management Framework provides a related structure for managing AI risks. In Pakistan, the State Bank of Pakistan's Enterprise ICT Governance and Risk Management Framework defines technology-governance expectations for financial institutions. These documents address different parts of governance. ISO/IEC 42001 focuses on organizational AI management, the NIST framework focuses on AI risk-management activities, and the State Bank of Pakistan framework addresses technology governance in financial institutions. In this paper, these requirements are used to support the design of controls for GenAI-assisted bank marketing. Consumer protection, deepfake transparency, intellectual property, and AI governance are mostly addressed as distinct topics in the current study. The aforementioned research clarify significant aspects of the issue, but they do not integrate them into a single operational model for GenAI-assisted marketing in Pakistan's banking industry. The next sections address this gap.

Table 1: *Mapping of common GenAI marketing risk classes in banking to Pakistan legal anchors and operational controls.*

Risk class in bank marketing	Pakistan legal anchor	Operational controls in the bank
Generated visuals, slogans, or campaign themes resemble a competitor's brand	Trade Marks Ordinance 2001	Brand constraint library, similarity screening, and legal approval for high-reach campaigns
Use of protected third-party images, text, music, or other creative assets in prompts or outputs	Copyright Ordinance 1962	Approved asset repository, rights metadata, and restrictions on uploading third-party material to external tools
Misleading marketing claims about rates, fees, eligibility, timelines, or product benefits	Competition Act 2010 deceptive marketing provisions and related guidance	Linking claims to approved product documents, compliance review gates, and audit logs for approvals
Synthetic testimonials, synthetic humans, or AI-generated voices used without appropriate disclosure	Consumer protection principles and deceptive marketing enforcement logic	Disclosure policy, creative labeling, approval gates for synthetic media, and customer complaint handling
Personalized offers generated through the use of sensitive or high-risk customer data	Draft Personal Data Protection Bill 2023 as a policy guide and sectoral expectations	Purpose limitation, data minimization, consent or lawful-basis mapping, and segmentation fairness testing
External deepfake advertisements or fake pages impersonating the bank	PECA Amendment Act 2025 and cybercrime enforcement pathways	Social monitoring, evidence capture, platform takedown, customer advisories, and coordination with fraud monitoring teams

The primary risk classes examined in this article are summarized in Table 1, which also links them to the pertinent Pakistani legal framework and bank-level controls. The chart also demonstrates that while certain controls are necessary before to publishing, others only become significant after the content has been made available. Before publishing, for instance, timely preparation, source-material selection, content review, and approval take occur. When deceptive or impersonated content later arises, monitoring and incident response are necessary.

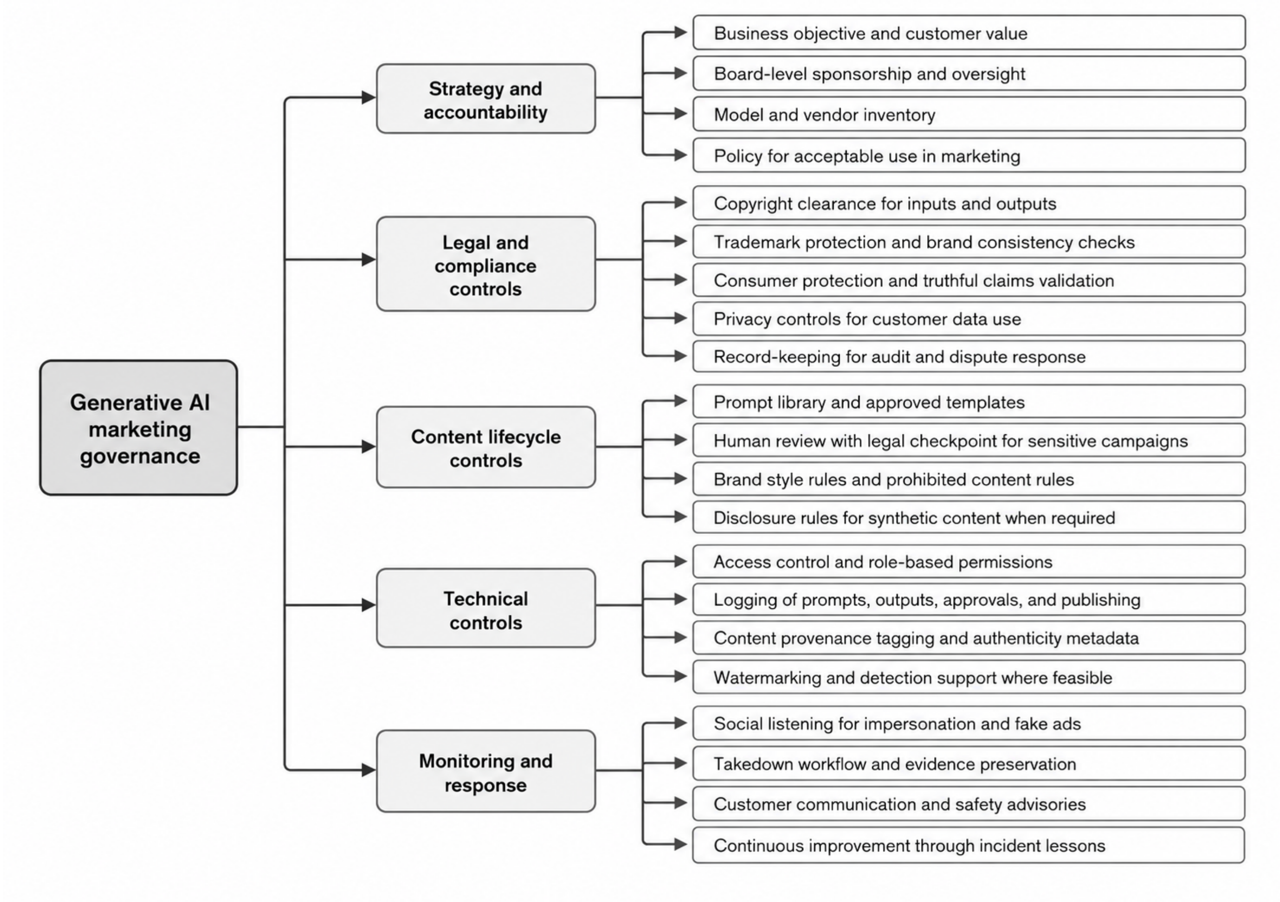

Figure 1: *Bank governance map for GenAI marketing in Pakistan.*

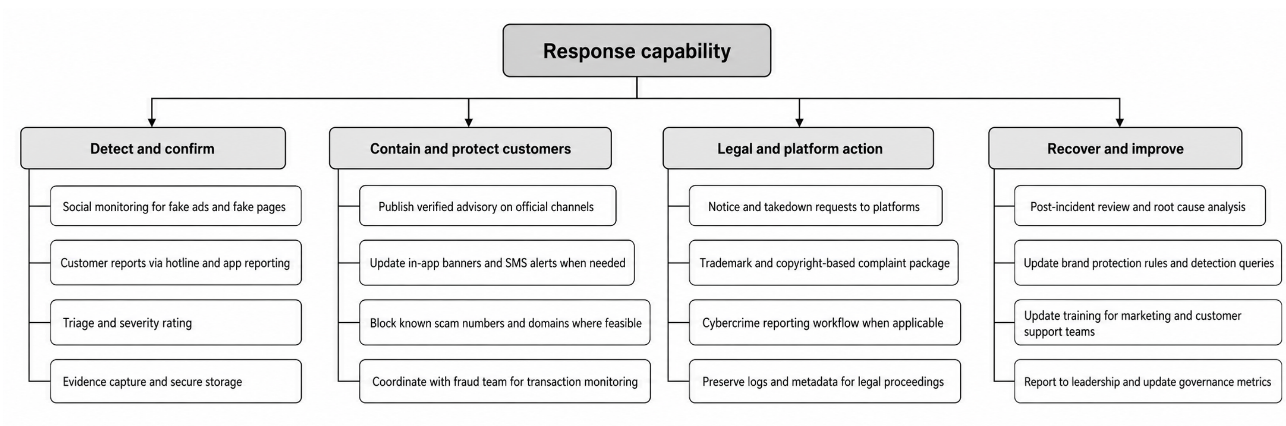

Figure 2: *Deepfake and impersonation response capability for banks.*

3. The Legal and Regulatory Framework for Bank Marketing with GenAI in Pakistan

The use of GenAI in bank marketing is covered by a number of Pakistani legal and regulatory frameworks. This article focuses on trademark protection, copyright, consumer protection, customer data, and cybercrime. These problems can occur prior to content publishing, during the usage of GenAI technologies, and following publication when phony or altered content shows up on the internet. Each topic is covered in the next subsections along with how it relates to bank marketing.

3.1. Trademark and Brand Identity

The legal foundation for trademark protection in Pakistan is provided by the Trade Marks Ordinance 2001. In situations where a mark may cause misunderstanding, misrepresent origin, or imply a misleading relationship, it offers remedies against unlawful use [4]. Banks that employ GenAI may have issues with both their own material and other parties abusing the bank's identity. A competitor's brand may be similar to a produced logo, slogan, campaign concept, or visual design. When an employee requests that a GenAI system adopt the style of another campaign, the identical problem may arise. Additionally, generated material can imply an unauthorized affiliation with a celebrity, influencer, or business partner. However, scammers could replicate a bank's trademarks and use them in phony commercials, social media profiles, or other promotional materials. Both situations are covered by trademark restrictions in this document. While external abuse is addressed by brand monitoring and impersonation response methods, internally created information is examined for resemblance and false connection.

3.2. Copyright in Marketing Assets and Training Data

Original works of literature and art are protected by the Copyright Ordinance of 1962. This might contain marketing writing, pictures, movies, software components, and other creative works [11], depending on the type of content. Both the raw data and the system's output may raise copyright issues for GenAI-assisted marketing. At the input stage, an employee may upload third-party content without first checking to see if its license permits such usage. This content may contain user-generated content, licensed media, competitor brochures, stock photographs, and other copyrighted elements. At the output step, the generated material may either closely resemble an existing work or reproduce protected expression. As a result, the framework makes a distinction between content that has been approved and content whose rights status is uncertain. It also keeps track of the provenance of the source content, any relevant permissions, and the pre-publication review procedure for the finished marketing asset.

3.3. Deceptive Marketing and Consumer Protection

The Competition Commission of Pakistan is responsible for advising and implementing the prohibitions against misleading marketing activities under the Competition Act 2010 [12]. Provincial consumer protection laws are also relevant. One example is the Punjab Consumer Protection Act 2005 and its subsequent amendments [13]. GenAI-generated marketing has the potential to be misleading even when the content is not totally false. A message may misrepresent eligibility, state the wrong fee, leave out an important requirement, or present a conditional benefit as if it were available to all clients. Similar problems might arise from automated advertising messages with ambiguous content, fake consumer experiences, and synthetic testimonials.These errors are important in the banking sector since customers may utilize promotional materials while choosing a financial product. As a result, the framework requires that product claims be checked against approved source materials before publication. This paper includes rates, fees, eligibility criteria, product limits, risk disclosures, and other information that may affect the customer's understanding of the offer.

3.4. Privacy and Customer Data

The proposed Personal Data Protection Bill 2023 [14] outlines principles for the processing, use, and sharing of personal data. These rules are applicable when banks use customer data for segmentation, customization, profiling, and automated messaging. GenAI can boost visibility when customer data is entered into an external service, combined with other data, stored by a vendor, or used to create personalized marketing content. As a result, the question is not just whether the data may be used for marketing, but also if all of the data placed into the system is actually required for that purpose. Access control, secure processing, data reduction, and purpose limitation are some of the suggested controls. The usage of consumer data in marketing should also be documented by the bank. Additional cybercrime problems may arise from unauthorized usage or access, especially when identity-related data is utilized to produce misleading material.

3.5. Cybercrime and Digital Impersonation

Pakistan's legal framework for illegal digital content, false information, online damages, and threats connected to impersonation includes the Prevention of Electronic Crimes Amendment Act 2025 [5]. This is pertinent to banks when AI-generated ads, bogus websites, or synthetic media are used to mimic an organization and trick clients. This kind of issue is not the same as a mistake in the bank's material. It's possible that the bogus content was produced and disseminated entirely outside of the bank's systems. The first step in responding in such a situation is to identify the material and preserve the evidence. After then, the bank may report the content, request its removal, work with the cybersecurity and fraud teams, and notify clients via proper channels. Section 6 presents the comprehensive response procedure. For instances of bank impersonation, it combines legal, cybersecurity, fraud management, and brand protection duties. Five legal requirements trademark and brand protection, copyright review, prohibition of deceptive communication, ownership of client data, and reaction to impersonation are necessary for GenAI-assisted bank marketing. The marketing team is not the only group in charge of these tasks. The distribution of responsibilities among the primary bank functions is displayed in Table 2.

Table 2: *Practical accountability model for GenAI use in bank marketing.*

Bank role	Primary responsibility	Accountability outputs
Chief Marketing Officer	Campaign objectives and channel governance	Campaign approval records, disclosure compliance, and brand consistency reports
Head of Compliance	Claim validation, consumer fairness checks, and policy enforcement	Compliance sign-off logs, exception approvals, and audit trails
Legal Counsel	Copyright and trademark review, dispute readiness, and takedown legal packages	Rights-clearance records, takedown documentation, and records prepared for dispute or litigation response
Chief Information Security Officer	Tool access control, logging, and integration with incident response	Access logs, model and vendor risk registers, and incident metrics
Data Protection Lead or Privacy Officer	Customer-data governance for personalization	Processing registers, retention schedules, and privacy assessments
Fraud Operations Lead	Response to deepfake-enabled scams and transaction-related fraud	Fraud alerts, loss metrics, and customer-protection actions

4. Research Design and Proposed Framework Approach

4.1. Methodological Stance

The proposed framework is developed using a design-oriented approach. Controls for GenAI-assisted bank marketing are created by first identifying the legal and governance concerns covered in the previous sections. The framework is developed in the study, but its efficacy is not experimentally tested. There are four phases in the method:

- Step 1. Determine the primary applications of GenAI in bank marketing, such as conversational marketing, campaign optimization, customization, and content generation.
- Step 2. Sort the legal and governance concerns related to these usage and connect them to Pakistan's appropriate enforcement interfaces and applicable legal responsibilities.
- Step 3. Create operational controls based on content-provenance procedures, banking technology-governance standards, and AI governance concepts. These controls are allocated to the pertinent bank operations as well as various phases of the marketing process.
- Step 4. Determine indications that may be utilized for audit and empirical assessment after applying the controls to a scenario-based banking case study.

GenAI use cases are followed by risk identification, control design, and implementation in the four processes. The paper makes no claims about how these measures lessen regulatory exposure, fraud, or legal challenges. It would be necessary to examine such impacts empirically.

4.2. Scope Boundaries

The paper focuses on marketing and consumer communications that banks create or oversee. When a bank's name, markings, or other brand assets are used for fraudulent advertising or impersonation, it also takes external abuse into account. This paper does not address the larger legal controversy surrounding the use of copyrighted content to train general-purpose GenAI models. Instead, the research concentrates on aspects of a bank's own marketing process that are under its control. These involve choosing sources, using GenAI tools, reviewing created content, approving it, publishing it, and dealing with misuse. The lifecycle controls, designated duties, and incident-response procedure described in the next sections are defined by these limits.

5. Integrated Compliance Framework for GenAI Marketing in Banks

The legal and governance controls are included into the GenAI marketing process in this paper. From content preparation to publishing and monitoring, the restrictions are implemented. The general governance structure and the locations of the primary controls are depicted in Figure 1. The State Bank of Pakistan's technology-governance standards [7], ISO/IEC 42001 management-system principles, and NIST AI risk-management ideas are all included into the framework.

5.1. Governance and Accountability Layer

When a bank uses GenAI for marketing, both management and operations must have clear accountability. The framework employs a cross-functional approval procedure and designates an executive owner for GenAI-enabled marketing. An inventory of the models, suppliers, equipment, and authorized use cases utilized in content creation is also necessary. These agreements align with the banking industry's requirements for risk-based technology management [15]. Basic governance records should also be kept by the bank. These include vendor due-diligence paperwork, a register of forbidden content, an acceptable-use policy, and escalation procedures for campaigns that need more investigation. The documents outline who gives the go-ahead, what is allowed and forbidden, and when escalation is required. ISO/IEC 42001 [10] places a similar focus on organizational policy, lifecycle management, risk handling, monitoring, and continuous improvement.

5.2. Copyright Compliance Controls for Marketing Content

A copyright evaluation is required for both the content entered into a GenAI system and the output produced by it. There are three sections to this control:

- Input governance: Employees should not send protected third-party marketing content to an external GenAI platform unless permitted by the license or authority. An authorized asset library including licensing information, permitted uses, and reuse restrictions may be maintained by the bank.
- Output governance: Generated material should be examined prior to publication. Additional evaluation may be necessary for product launches, influencer material, national advertisements, and other high-exposure initiatives. Depending on the asset, the evaluation may include reverse-image search, text-similarity verification, and brand assessment. These tests do not serve as a legal evaluation in situations where copyright depends on the degree of likeness and protected expression [11].
- Contractual governance: Agreements with GenAI vendors should outline who is responsible for the generated outputs and how they might be used. Included should be data storage, timely retention, confidentiality, and the potential to use bank-provided data for model training. These issues also relate to the technology outsourcing and risk governance needs of financial organizations [16].

5.3. Trademark and Brand Protection Controls

Content created by the bank and unapproved use of the bank's identity by other parties can both result in trademark issues. We use three controls to deal with these issues:

- Brand constraints: Approved brand assets, typography, tone, and design guidelines should be used by GenAI products. This lessens the possibility that produced content would match the mark or visual identity of a rival.
- Confusion review: Before being published, generated information should be examined for any unapproved associations or similarities to rival identities. The analysis should also take into account the possibility of a consumer misinterpreting the communication's origins.
- External brand protection: The bank should have a procedure in place for spotting phony pages, ads, and other unapproved uses of its name. Monitoring public channels, preserving evidence, reporting false content, and reporting the event to the legal, compliance, security, and fraud departments are all part of this procedure.

The legal foundation for action against infringing uses of marks and statements that might be confusing is provided by the Trade Marks Ordinance 2001 [4]. This criteria is applied to GenAI-assisted marketing through these rules.

5.4. Consumer Protection, Truthful Claims, and Disclosure

GenAI may provide inaccurate product terms, utilize out-of-date pricing data, or omit offer conditions. Because clients may rely on this information when selecting a financial product, these mistakes are significant in the banking industry. Because of this, before being published, statements about rates, prices, eligibility, deadlines, guaranties, waivers, prizes, or risk disclosures should be verified with an authorized product source. The approval record should include the source document, reviewer, and timestamp. The Competition Act 2010 [12] provides the legal basis for action against misleading advertising and representations. Consumer protection laws are also relevant when warnings are inadequate or representations result in incorrect expectations about a financial product [13]. Furthermore, the use of synthetic endorsements, synthetic people, and deepfake-like content must be reported. The disclosure should be clear from the channel in which it occurs. Previous advertising research [2] indicates that disclosure can impact client assessment and trust.

5.5. Privacy and Fairness in Personalized Marketing

Personalized marketing may employ transaction-derived data, customer behavior, demographic information, and digital interaction patterns to decide which offers are shown to certain customers. Safe processing, access control, data minimization, and purpose limitation are all applied to these processes by the framework. Pakistan's proposed Personal Data Protection Bill 2023 [14] may serve as the basis for internal rules on the use of customer information. Evaluation of the targeting process is also required. For example, a model can target a certain demographic group with an offer or utilize proxy factors to reject otherwise qualified clients. For sensitive or high-impact advertisements, the method includes a fairness evaluation. The campaign's variables, targeting rationale, eligibility requirements, and approval decision should all be documented by the bank. These documents can be utilized in the future to examine the reasons behind the inclusion or exclusion of a certain client category.

5.6. Content Provenance and Authenticity Controls

A bank can demonstrate the origin and approval process of an official marketing asset by using provenance records. According to the framework, banks must hold onto authorized campaign assets and associated authenticity data. Additionally, a useful method for identifying official messages should be provided to customers. An industry standard for connecting provenance information to digital assets is provided by C2PA [17]. Provenance credentials are not supported by all external platforms. The bank may store the provenance record internally if such credentials cannot be shown or kept. Later on, these data may be utilized for customer verification, evidence retention, dispute resolution, and removal requests pertaining to material that has been altered or impersonated.

6. Deepfake Incident Response and Legal Accountability Workflow

When bank brand, executives, employees, or clients are used in deepfake or impersonation content without permission, they must have a clear reaction. Because false content may spread before the bank can check or remove it, the reaction should be prepared ahead of time. The suggested workflow is shown in Figure 2. It addresses fraud monitoring [5], platform reporting or removal, customer communication, and evidence retention. Financial fraud, disinformation, identity theft, and reputational damage have all been linked to deepfake misuse [18]. Any suspicious material should first be noted by the bank and kept on file. The matter can then be reported to the relevant fraud, cybersecurity, legal, and customer-communication departments. Depending on the situation, the bank may submit a platform complaint or takedown request, notify customers through formal channels, monitor related fraud activity, and, if required, submit legal or cybercrime complaints. Removing the online material is only one part of the response, as some customers may have already received or acted upon it. The Prevention of Electronic Crimes Amendment Act 2025 [5] is part of Pakistan's legal framework for illegal online content and digital impersonation. In Figure 2, the bank's current fraud, cybersecurity, legal, and customer-communication processes are integrated with this legal framework. For consumer warning, escalation, evidence retention, and follow-up action, the workflow provides an organized procedure.

7. Banking Sector Case Study for Pakistan

7.1. Scenario Description

Consider a Pakistani mid-sized commercial bank planning a digital campaign for a new debit card and youth account. In this scenario, campaign writing, Urdu-English slogans, product descriptions, and lifestyle images are created using GenAI. Additionally, the campaign employs a chatbot-style landing page to respond to inquiries about the product and point prospective buyers toward the account sign-up procedure. This example situation illustrates how the previously described rules would be implemented in a bank marketing campaign.

7.2. Where Legal Issues Emerge

- Copyright: To find stylistic trends, the marketing team suggests feeding competitor campaign posters into a GenAI program. There is no clear set of rights for this usage. As a result, the team chooses content from an authorized asset library with proven rights clearance [11].
- Trademark: One created debit card design is similar to a competitor's product's identifiable layout. The design is sent for legal assessment once the similarity check finds the likeness. To minimize potential consumer misunderstanding and trademark exposure, it is changed prior to publication [4].
- Deceptive marketing: The account has no yearly cost, according to the model's output. Only a restricted fee waiver is offered by the real product. Before being published, the statement is verified against the official schedule of charges and revised. The approval record [12] retains the original document and review judgment.
- Privacy and fairness: The suggested strategy uses behavioral cues and transaction proxies to target students. Prior to using these signals, their need and purpose are examined, and the targeting model is examined for unjust exclusion. Additionally, the bank keeps track of the targeting criteria and evaluates whether groups that are equally qualified would be left out without a justification. For this portion of the scenario, a policy reference is provided by the draft data-protection framework [14].
- Readiness for deepfake responses: Scammers release a phony promotional video with a synthetic voice within two weeks of the campaign's debut. In exchange for viewers' card information, the video offers quick cash awards. In the hypothetical situation, the bank notifies its fraud-monitoring staff, keeps the video as proof, files takedown

requests, and notifies clients via formal channels. The reporting and evidence-preservation measures are pertinent to the cybercrime-law context [5].

The campaign's many points are covered by the examples. While product claims and targeting must be reviewed before to publishing, copyright and trademark concerns arise during the preparation of material. The deepfake problem happens after launch and necessitates a different approach that includes consumer communication and fraud monitoring.

7.3. Measurable Indicators for Audit and Continuous Improvement

If the framework is implemented, the bank may verify that the necessary controls are being followed by using its current marketing, compliance, and incident data. Potential markers include:

1. percentage of campaigns that have full files for rights clearance.

   A item number of marketing claims that have been verified by official product papers.

   A item quantity of goods with synthetic material that have the proper disclosure labels.

   A item The time it takes to identify and remove impersonation events.

   A item percentage of personnel who are qualified to utilize GenAI for marketing.

   The quantity of consumer complaints related to deceptive advertising or marketing.

These metrics evaluate record-keeping and execution rather than the framework's overall efficacy. They can be examined throughout time to find processes that need to be revised or controls that are not being followed. The management-system and risk-management principles previously discussed [10] align with this kind of monitoring. It is not possible to deduce a decrease in operational or legal risk from these data alone.

8. Discussion

There are two ways that GenAI impacts bank marketing. While external actors can use the same technology to mimic bank communications, banks can utilize it to create authentic marketing content. This difference is crucial since instant-payment services, fintech partnerships, digital onboarding systems, mobile banking applications, and other internet channels are being used to offer bank marketing. These channels can also be used to disseminate modified material and fake ads. The legal framework for addressing illegal digital content and associated online damages in Pakistan includes the PECA amendments [5]. Because of this, managing GenAI-assisted marketing cannot be restricted to reviewing the finished product. Additionally, a bank must determine what information may be submitted into GenAI tools, who is permitted to use them, how product claims are validated, and what permission records need to be maintained. When fraudulent content is produced outside of the bank, a different procedure is required. Teams from marketing, law, compliance, cybersecurity, privacy, and fraud are involved in these operations. Response teams also face a practical challenge as a result of deepfake occurrences. Customers may need to be alerted and fraudulent content may need to be swiftly deleted, but a takedown request must still be backed up by proof. As a result, the bank should keep the information safe, note the cause of the escalation, and record any requests for removal or other actions. Unauthorized reproduction or imitation of an identified person raises similar issues, especially when privacy or dignity may be compromised. By having controls in place at the point where the associated risk manifests, the framework tackles these problems. When source material and created assets are being prepared, copyright and trademark checks begin. While customer-data controls are in place for customization and targeting, product claims are verified prior to publishing. The incident-response procedure is applied when external impersonation emerges after publishing, and provenance records facilitate subsequent verification. Legal review is thus considered more than just the last stage of approval.

8.1. Limitations

This paper provides a conceptual framework and explains its implementation through a qualitative case study of the banking sector. It doesn't demonstrate how using the framework lowers the risk of fraud, litigation, regulatory exposure, or harm to customers. Evidence gathered over time from banks, consumers, digital platforms, and pertinent enforcement agencies would need to be used to assess such impacts. Additionally, practical implementation may vary from bank to bank. Banks vary in their technological resources and governance capabilities, certain systems do not accept provenance credentials, and local-language deepfake-detection tools may be scarce. As a result, the case study shows how the controls may be used without confirming their efficacy. Future research should evaluate whether the controls are used as planned and if they result in quantifiable improvements in practice.

9. Conclusion

Although GenAI may be used for content creation, customization, and client engagement in bank marketing, its application also brings up concerns about copyright, trademarks, false claims, customer data, synthetic media, and bank impersonation.

These concerns must be taken into account in Pakistan together with consumer and competition legislation, cybercrime regulation, data protection policy, financial technology governance, and intellectual property law. We presented a compliance framework for GenAI-assisted bank marketing in Pakistan in this article. At various phases of the marketing process, the framework places rights clearance, brand review, product claim verification, customer data controls, disclosure, content provenance, and deepfake reaction. The use of these controls was shown through a scenario-based banking case study, and a set of indicators was established for further audit and assessment. The paper does not demonstrate that putting the framework into practice will lessen regulatory risk, fraud, or litigation. Such impacts need to be evaluated empirically. The suggested approach gives banks an organized method for allocating accountability, documenting significant choices, and implementing the necessary controls during GenAI-assisted marketing.

Author Declarations

Author Contributions (CRediT): Madiha Awais: Conceptualization, Methodology, Investigation, Literature Review, Data Curation, Formal Analysis, Visualization, Writing - Original Draft. The author reviewed and approved the final manuscript.

Funding: No external funding was received for this research.

Data Availability Statement: No new datasets were generated or analyzed in this paper.

Acknowledgments: The author would like to thank the Center for Emerging Networks & Technologies (CENT) Lab at the University of Central Punjab (UCP), Lahore, Pakistan, for technical support and constructive feedback.

Conflicts of Interest: The author declare no conflicts of interest.

Ethics Statement: Not applicable.

Declaration of Generative AI: During the preparation of this work, the author used generative AI tools only for language editing and proofreading, where applicable. The authors reviewed and edited the content and take full responsibility for the published article.

References

[1] Duivenvoorde, B. (2025). Generative AI and the future of marketing: A consumer protection perspective. Computer Law & Security Review, 57, 106141. https://doi.org/10.1016/j.clsr.2025.106141

[2] Whittaker, L., Mulcahy, R., Russell-Bennett, R., Letheren, K., & Kietzmann, J. (2025). Examining consumer appraisals of deepfake advertising and disclosure: Show deepfakes as "real life" or say they're "just fantasy"? Journal of Advertising Research, 66(1), 113–134. https://doi.org/10.1080/00218499.2025.2498830

[3] Sutrisno, G. B. (2025, January 30). WFA finds copyright and IP issues are stalling GenAI in marketing. Marketing-Interactive. https://www.marketing-interactive.com/wfa-finds-copyright-and-ip-issues-are-stalling-genai-in-marketing

[4] Government of Pakistan, Ministry of Law and Justice. (2001). Trade Marks Ordinance, 2001 (Ordinance No. XIX of 2001). Pakistan Code. https://pakistancode.gov.pk/

[5] Government of Pakistan. (2025). Prevention of Electronic Crimes (Amendment) Act, 2025 (Act No. II of 2025). The Gazette of Pakistan, Extraordinary, January 29, 2025. https://na.gov.pk/uploads/documents/679b243193585_457.pdf

[6] State Bank of Pakistan. (2017). Enterprise Technology Governance & Risk Management Framework for Financial Institutions. Annex to BPRD Circular No. 05 of 2017, Banking Policy & Regulations Department. https://www.sbp.org.pk/bprd/2017/C5-Annex.pdf

[7] Tabassi, E. (2023). Artificial Intelligence Risk Management Framework (AI RMF 1.0). NIST AI 100-1. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.AI.100-1

[8] Chesterman, S. (2025). Good models borrow, great models steal: Intellectual property rights and generative AI. Policy and Society, 44(1), 23-37. https://doi.org/10.1093/polsoc/puae006

[9] Budd, F., Gray, L., & Aries, N. (2025). The impact of AI on trade mark law and practice. Trade Marks Laws and Regulations Report 2025, International Comparative Legal Guides (ICLG), Global Legal Group. https://iclg.com/practice-areas/trade-marks-laws-and-regulations/01-the-impact-of-ai-on-trade-mark-law-and-practice

[10] International Organization for Standardization & International Electrotechnical Commission. (2023). ISO/IEC 42001:2023: Information technology-Artificial intelligence-Management system. ISO. https://www.iso.org/standard/42001.html

[11] Government of Pakistan, Ministry of Law and Justice. (1962). Copyright Ordinance, 1962 (Ordinance No. XXXIV of 1962). Pakistan Code. https://pakistancode.gov.pk/pdffiles/administrator5d255d1f44b50b65d6a3e87a2e0d3fee.pdf

[12] Government of Pakistan. (2010). Competition Act, 2010 (Act No. XIX of 2010). Pakistan Code. https://pakistancode.gov.pk/pdffiles/administratore1b5ab79c2c1975670e6aa7fe57e57d6.pdf

[13] Government of Punjab. (2005). The Punjab Consumer Protection Act 2005 (Pb. Act II of 2005). https://pccmdpunjab.gov.pk/custom/mateen/pdf/ruleregulation/20-Punjab%20Consumer%20Protection%20Act%202005.pdf

[14] Ministry of Information Technology and Telecommunication, Government of Pakistan. (2023). Personal Data Protection Bill, May 2023 (Final Draft). https://www.moitt.gov.pk/Legislations

[15] State Bank of Pakistan. (2017). BPRD Circular No. 05 of 2017: Enterprise Technology Governance & Risk Management Framework for Financial Institutions. Banking Policy & Regulations Department, May 30, 2017. https://www.sbp.org.pk/circulars/bprd-circular-no-05-of-2017

[16] State Bank of Pakistan. (2019). BPRD Circular No. 06 of 2019: Framework for Risk Management in Outsourcing Arrangements by Financial Institutions. Banking Policy & Regulations Department, December 17, 2019. https://www.sbp.org.pk/circulars/bprd-circular-no-06-of-2019

[17] Coalition for Content Provenance and Authenticity. (2025). Content Credentials: C2PA Technical Specification, Version 2.4. https://spec.c2pa.org/specifications/specifications/2.4/specs/C2PA_Specification.html

[18] Romero-Moreno, F. (2025). Deepfake detection in generative AI: A legal framework proposal to protect human rights. Computer Law & Security Review, 58, 106162. https://doi.org/10.1016/j.clsr.2025.106162