FIDELITY AND CYBERCRIME: AN ANALYSIS OF INCLUSIVITY OF CYBERCRIME UNDER FIDELITY GUARANTEE INSURANCE IN INDIA

Abhay A V, CMR University School of Legal Studies

ABSTRACT

In India the traditional general insurance safeguards an insured from the financial losses suffered due to damage to assets, health emergencies or liability claims. The general insurance excludes the protection of financial loss suffered from theft, robbery or unfaithfulness of the employee in business operation and it is protected under Fidelity Guarantee Insurance. Organizations increasingly face risks arising from employee misconduct carried out through digital means, such as unauthorized system access, data theft, online fraud, and manipulation of electronic records. Simultaneously in business or companies cyber fraud or cyber theft have emerged as the concerning risk to be protected from and the best possible way is to procure an additional policy such as cyber insurance apart from Fidelity Guarantee Insurance.

This paper will dive into the matrix of Fidelity Guarantee Insurance and understand the expansive coverage it holds by analyzing and reviewing case notes and study materials. Furthermore, the empirical part of the paper will be the inclusivity of the cybercrime under Fidelity Guarantee Insurance. This can be dealt by undergoing deep analysis of regulations governing Fidelity Insurance and Cybercrime Insurance and the emphasis on the policy wording as addressed by the Indian courts. Moreover, this paper will delve into the nuances and procedures as to the inclusivity of cybercrime under Fidelity Insurance to understand how cybercrime has been integrated as part of the Fidelity Insurance.

Keywords: Fidelity Guarantee Insurance, Cybersecurity, Cyber Insurance, Regulation, Inclusivity.

INTRODUCTION

The Indian insurance framework draws a foundational distinction between general insurance which covers loss arising from damage to assets, liability claims, and health contingencies and the more specialised class of Fidelity Guarantee Insurance, which protects employers from direct pecuniary losses caused by acts of fraud, dishonesty, or breach of faith by their employees.[1] General insurance policies, as a matter of standard market practice and regulatory design, expressly exclude losses attributable to employee misconduct, relegating such risks to the Fidelity Guarantee framework. A standard Fidelity Guarantee Insurance Policy such as that issued by SBI General Insurance Company Limited indemnifies the employer against direct pecuniary loss arising from any act of fraud or dishonesty committed by an employee during the continuance of the policy, provided the loss is discovered within twelve calendar months of the policy's expiration or the employee's death, dismissal, or retirement.[2] The definitional framework of such policies covering fraud, dishonesty, forgery, and embezzlement was developed in an era of predominantly physical commercial activity.

The rapid digitisation of business operations has, however, produced a new category of employee misconduct: cybercrime. Employees now commit financial fraud through unauthorised access to computer systems, manipulation of electronic records, online impersonation, and digital embezzlement. The current Indian legal landscape governing the indemnification of cybercrime is 'Cyber Insurance'. Cyber insurance is nothing but insurance designed to guard businesses from the potential effects of cyber-attacks. It helps an organisation mitigate risk exposure by offsetting costs, after a cyber-attack/breach has happened. To simplify, cyber Insurance is designed to cover the fees, expenses and legal costs associated with cyber breaches that occur after an organisation has been hacked or from theft or loss of client/employee information[3].

In India, Cyber Insurance is regulated under the general insurance policy and enactment thus narrowing the scope of the regulatory mechanisms of Cyber Insurance in India. The question of whether such acts of cybercrime fall within the indemnification obligation of a Fidelity Guarantee insurer is one of pressing practical and doctrinal significance, yet it remains

[1]Insurance Regulatory & Development Authority of India, *Guidelines on Standard Fire and Special Perils Policy* (2021); K.S.N. Murthy & K.V.S. Sarma, *Modern Law of Insurance in India* 42–45 (5th ed. 2013).
[2]SBI Gen. Ins. Co. Ltd., *Fidelity Guarantee Insurance Policy* cl. 1 (Standard Form).
[3]Data Sec. Council of India, *Cyber Insurance in India: Mitigating Risks Amid Changing Regulations & Uncertainties* 12 (2019).

underexplored in Indian legal scholarship. Furthermore, the Apex Court of India has held that the strict interpretation of exclusion clauses in insurance policies is a principle which must not be overlooked[4] which makes that the exponential growth of the cyber crime and Cyber Insurance questionable in the definition of the general insurance.[5]

This paper advances the argument that a purposive interpretation of the definitional categories of Indian Fidelity Guarantee Insurance policies informed by the Information Technology Act, 2000,[6] relevant judicial pronouncements, and comparative insurance law supports the inclusion of employee-perpetrated cybercrime within fidelity coverage, subject to conditions. The paper also identifies the structural limitations and coverage gaps that necessitate regulatory reform.

NATURE AND SCOPE OF FIDELITY GUARANTEE INSURANCE IN INDIA

Fidelity Guarantee Insurance occupies a distinctive position within the Indian insurance taxonomy. Unlike general insurance products that indemnify against externally generated risks, fidelity insurance addresses the internal risk of employee infidelity the possibility that persons entrusted with the employer's assets, systems, or confidential information will abuse that trust for personal gain. The philosophical underpinning of fidelity insurance, as articulated by McNamee, is that the loss caused by employee dishonesty should fall on the employer as a risk of the business enterprise, since the employer is better positioned to prevent such losses through careful selection and supervision of staff.[7]

The principal obligations under a standard fidelity policy are: (a) indemnification of the insured employer against direct pecuniary loss; (b) arising from an act of fraud, dishonesty, forgery, or embezzlement; (c) committed by an employee; (d) during the continuance of the policy and uninterrupted service; and (e) discovered within the prescribed discovery period. Each element raises interpretive questions when applied to digitally executed misconduct.

The policy defines "fraud" as obtaining a pecuniary advantage through unfair or wrongful means; "dishonesty" as a breach of faith resulting in pecuniary loss to the employer; "forgery" as the fraudulent alteration or circulation of a document to obtain possession of

[4]*Oriental Insurance Co. Ltd. v. Muni Mahesh Patel*, (2006) 7 S.C.C. 174 (India).
[5]Insurance Act, 1938, § 2(6B) (India).
[6]Information Technology Act, 2000, §§ 43, 66, 66C, 66D, 72A (India).
[7]Charles R. McNamee, Fidelity Insurance—For Whose Benefit?, 1965 Ins. Couns. J. 125, 126.

money or goods; and "embezzlement" as the misappropriation of monies or goods that have come into the employee's possession before passing to the employer[8]. The exclusions under standard policies are equally significant: they exclude losses discovered more than twelve months after the termination of the guarantee or the employee's service, losses caused by an employee after discovery of previous fraud, stock-taking shortages not caused by fraud or dishonesty, liability arising from violation of government regulations, and losses arising outside India.

The Indian courts have consistently applied the principle that exclusion clauses in insurance policies are to be construed narrowly, while coverage clauses are to be interpreted broadly in favour of the insured.[9] Provided it is the duty of the insurer to plead and lead cogent evidence to establish the application of such a clause, and the evidence must unequivocally establish that the event sought to be excluded is specifically covered by the exclusionary clause[10]. This canon of interpretation provides an important foundation for extending fidelity coverage to cybercrime, particularly where the act of misconduct satisfies the definitional elements of fraud or dishonesty, regardless of the digital medium through which it is affected.

EMPLOYEE CYBERCRIME: FORMS AND FREQUENCY

Employee perpetrated cybercrime constitutes a major and growing subset of overall cybercrime exposure for organisations. Globally, it is estimated that as many as seventy to eighty percent of cyber insurance claims result from human error or malfeasance, with insider threats by privileged users those with unfettered access to an organisation's network, devices, and servers representing the most significant category.[11] In the Indian context, the rapid adoption of digital financial systems across banking, financial services, insurance, retail, and public administration has dramatically expanded the surface area of employee directed cyber risk. The principal forms of employee cybercrime relevant to fidelity insurance claims include: (i) unauthorised access to and manipulation of electronic financial records to divert funds; (ii) phishing and business email compromise where employees, acting either as perpetrators or facilitators, cause fraudulent transfers; (iii) data theft the misappropriation of the employer's proprietary or confidential data for personal benefit or for the benefit of a third party; (iv)

[8]Mark Camillo, Cyber Risk and the Changing Role of Insurance, 2(1) J. Cyber Pol'y 53, 54–55 (2017).
[9]*National Insurance Co. Ltd. v. Ishar Das Madan Lal*, (2007) 4 S.C.C. 105 (India).
[10]*Texco Mktg. P. Ltd. v. TATA AIG Gen. Ins. Co. Ltd.*, (2023) 1 S.C.C. 428 (India).
[11]*Supra* note 8, at 57.

identity theft and impersonation, typically facilitated by the employee's privileged access credentials; and (v) manipulation of accounting software to conceal embezzlement.

The Information Technology Act, 2000 (ITA) provides the primary legislative framework governing these acts in India. Section 43 imposes civil liability for unauthorised access to computer systems; Section 66 criminalises computer-related offences; Section 66C criminalises identity theft; Section 66D criminalises cheating by impersonation using computer resources; and Section 72A imposes liability for disclosure of information in breach of lawful contract. These provisions indicate that the legislature has recognised the pecuniary character of cybercrime and has created legal remedies corresponding to the traditional forms of fraud and dishonesty that fidelity insurance was designed to address.

A body corporate that fails to implement and maintain reasonable security practices is additionally exposed to liability under Section 43A of the ITA.[12] This can be enumerated with catena of judgments where in several such cases, the adjudicating officer assessed whether banks had adhered to the "Know Your Customer" (KYC) norms and guidelines issued by the Reserve Bank of India to prevent banking fraud. Where deficiencies in compliance were identified particularly in situations where lapses enabled fraudsters to gain access to a complainant's bank account a presumption of negligence was drawn against the bank in handling "sensitive personal information." This failure to implement reasonable security practices attracted liability for compensation under Section 43A, even in instances where the complainant had partly contributed to the breach by responding to phishing emails or sharing information with third parties. Such cases clearly fall within the ambit of Section 43A, which extends protection to financial information including bank account details, credit or debit card data, and other payment instrument information by treating it as sensitive personal data and imposing obligations on body corporates to safeguard it. The adjudicating officer's approach merits appreciation for imposing a heightened duty of care on banks to protect the informational privacy of their customers. Given their access to and control over highly sensitive financial data, banks are expected to maintain robust mechanisms to prevent fraud. Their failure to do so justifies not only compensatory relief for the losses suffered but also the imposition of

[12]Information Technology Act, 2000, § 43A (India); Insurance Regulatory & Development Authority of India, *Guidelines on Information and Cyber Security for Insurers* (2017).

punitive damages.[13]

From an insurance perspective, the failure to maintain adequate security can affect the insured's ability to claim under a fidelity policy, particularly where such failure constitutes a breach of the additional conditions typically warranted under the policy such as dual control accounting systems, regular internal audits, and daily cash book reconciliation.

CYBER INSURANCE, PROCEDURAL OBLIGATIONS, AND THE PATH TOWARDS AN INTEGRATED FRAMEWORK

A. Adjudicatory Jurisprudence

A series of adjudication orders passed by the Adjudicating Officer (Information Technology), Government of Maharashtra, under Section 46 of the Information Technology Act, 2000, have progressively developed the body corporate's security obligations in a manner directly relevant to the fidelity insurance context. These decisions collectively establish that financial institutions and other body corporates handling sensitive personal data, including payment instrument details, bear a non-delegable duty of reasonable security that is enforceable both through civil compensation and, in aggravated cases, punitive damages.

In Ravindra Gunale v. Bank of Maharashtra & Vodafone India Ltd., the Adjudicating Officer held both the bank and the telecom service provider jointly liable for failing to implement adequate verification procedures for the issuance of a duplicate SIM card, which enabled fraudulent banking transactions.[14] In Ram Techno Pack v. State Bank of India, the bank was held liable under Section 43A for inadequate internet banking security controls that permitted unauthorised online transactions, with the order applying the SPDI Rules, 2011, to confirm that financial account information attracts the highest standard of security protection.[15] In Srinivas Signs v. IDBI Bank, the Adjudicating Officer affirmed that the security obligation is continuous and demands progressive upgrades in line with evolving threats, holding that compliance with past standards does not discharge the duty where more effective security

[13]Divij Joshi, *A Review of the Functioning of the Cyber Appellate Tribunal and Adjudicatory Officers under the IT Act*, Ctr. for Internet & Soc'y (June 16, 2014).
[14]*Ravindra Gunale v. Bank of Maharashtra & Vodafone India Ltd.*, Adjudication Order (Feb. 20, 2013) (Adjudicating Officer, Govt. of Maharashtra) (India).
[15]*Ram Techno Pack v. State Bank of India*, Adjudication Order (Feb. 22, 2013) (Adjudicating Officer, Govt. of Maharashtra) (India).

measures have since become available.[16]

In Raju Dada Raut v. ICICI Bank, the officer awarded compensation on the basis that ICICI Bank failed to implement adequate transaction monitoring and verification systems proportionate to the specific nature and volume of sensitive data it handled.[17] In Pravin Parkhi v. SBI Cards and Payments Services Pvt. Ltd., the officer affirmed that financial institutions have a heightened duty of care in the protection of payment instrument data, extending to proactive rather than merely reactive security measures.[18] Taken together, these five adjudication orders establish a cohesive jurisprudence of digital security negligence that is directly applicable to the fidelity insurance context: where an employer's failure to implement adequate internal security controls created the conditions under which an employee was able to execute digital fraud, the insurer may legitimately invoke that failure as a basis for contesting the fidelity claim or reducing the quantum of indemnification.

B. Procedural Obligations in Fidelity Claims Involving Cybercrime

The procedural conditions precedent to a valid fidelity claim assumes distinctive and challenging dimensions when the underlying loss arises from a digital act. Under the standard SBI General Insurance Fidelity Guarantee Policy, the insured is required, upon discovering any act or circumstance that may give rise to a claim, to forthwith give written notice to the insurer, immediately take steps to prevent further loss, and provide all proof, information, and evidence as the company may require.[19] The obligation to provide all proof and evidence as the insurer may require must be read against the admissibility requirements of Section 65B of the Indian Evidence Act, 1872, as authoritatively interpreted by the Supreme Court in Anvar P.V. v. P.K. Basheer and subsequently refined in Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal.[20] Electronic records including server logs, digital transaction histories, access credentials, and email communications constitute the primary evidence of employee cybercrime, yet their admissibility as secondary evidence is conditional upon the provision of

[16]*Srinivas Signs v. IDBI Bank Ltd.*, Adjudication Order (Feb. 18, 2014) (Adjudicating Officer, Govt. of Maharashtra) (India).
[17]*Raju Dada Raut v. ICICI Bank Ltd.*, Adjudication Order (Feb. 13, 2013) (Adjudicating Officer, Govt. of Maharashtra) (India).
[18]*Pravin Parkhi v. SBI Cards & Payments Servs. Pvt. Ltd.*, Adjudication Order (Dec. 30, 2013) (Adjudicating Officer, Govt. of Maharashtra) (India).
[19]SBI Gen. Ins. Co. Ltd., *Fidelity Guarantee Insurance Policy* conditions 1(a)–(c) (Standard Form); Insurance Act, 1938, § 64VB (India); Insurance Regulatory & Development Authority of India (Protection of Policyholders' Interests) Regulations, 2017, reg. 9.
[20]*Anvar P.V. v. P.K. Basheer*, (2014) 10 S.C.C. 473 (India).

a Section 65B certificate. The Court in Arjun Panditrao confirmed that this certificate is a condition of admissibility and not merely a formality and its absence is fatal to the evidential basis of the claim. Insured employers must therefore instruct their information technology departments to preserve and certify all relevant digital records immediately upon discovering the misconduct, rather than waiting until the forensic investigation is complete.

The obligation to prosecute the defrauding employee to conviction, where required by the insurer, triggers a further set of procedural demands in the cybercrime context. A complaint under the IT Act or the BNS must be filed with the relevant cybercrime investigation authority, and the insured must cooperate fully in providing digital forensic evidence and technical testimony. The insurer's subrogation rights, which arise upon payment of the fidelity claim, extend to the full range of legal remedies available against the defrauding employee under both the ITA and the IPC.[21]

The IRDAI's regulatory requirement that claims be settled or rejected within thirty days of receipt of all relevant documents must be read realistically in the cybercrime context.[22] A digital forensic investigation cannot ordinarily be completed within thirty days. The insured should therefore submit a preliminary notice of claim immediately upon discovery and maintain ongoing communication with the insurer as the investigation progresses. Failure to observe the notice condition with delays may provide a basis for the insurer to decline the claim on a procedural ground, regardless of its substantive merits.

C. The Exhortation for an Integrated Fidelity-Cyber Framework

The analysis in this Part demonstrates that the relationship between fidelity guarantee insurance and cyber insurance in India is characterised by a structural disarticulation two distinct policy frameworks addressing overlapping risks without any regulatory mechanism for their coordination. This disarticulation creates both a protection gap and a procedural burden for insured employers, who must navigate the conditions precedent and evidential requirements of both frameworks simultaneously while managing the reputational, operational, and regulatory consequences of a cybersecurity incident.

[21] *Supra* note 7, at 127–28.
[22] Insurance Regulatory & Development Authority of India (Protection of Policyholders' Interests) Regulations, 2017, reg. 9.

Notwithstanding the analysis ongoing in this section, the standard fidelity policies contain certain features that may hinder the claims arising from the cybercrime. The fidelity insurance claim requires the loss be "directly" pecuniary is one of the major setbacks in cases involving cybercrimes such as data theft in which case the direct loss here is intangible asset i.e., "data" rather than physical goods or money. The absence of policy wordings/language creates vagueness in determining the coverage under the fidelity claims. Next, normally in the cases of cybercrime the knowledge of the crime comes to the attention after the period of 170 days and this discovery nearly doubles where the attack involves an insider[23]. This arises problems in the fidelity claims where the clauses are predominantly requires discovery within twelve months of policy expiration or employee termination. Lastly, other additional conditions which is pre-drafted in the fidelity claims such as dual control accounting, regular audits, daily cash book reconciliation are standard mandates and the cybersecurity concerned obligations which is necessary to mitigate the risks i.e., two-factor authentication, endpoint survey, network monitoring etc are not addressed. This poses risk to the insured as the insurer can anytime reject the claim stating the failure to meet the standard mandates.

The global trajectory of the cyber insurance market pointed towards the convergence of fidelity and cyber risk within integrated insurance frameworks, the extension of cyber wordings across traditional policy classes, and the institutionalisation of the insurance industry as a private regulator of cybersecurity standards[24], provides both the model and the progress for regulatory reform in India. The IRDAI should consider mandating a cyber endorsement within all standard fidelity guarantee policies, explicitly extending coverage to digitally executed fraud, dishonesty, forgery, and data misappropriation, updating the additional warranty conditions to incorporate contemporary cybersecurity obligations, and establishing a clear coordination mechanism between fidelity and cyber insurance for losses arising from employee cybercrime. Such reform would ensure that the protective purpose of fidelity insurance is preserved in an era where the instruments and consequences of that infidelity have fundamentally changed.

CONCLUSION

The convergence of employee dishonesty with digital means presents one of the most

[23] *Supra* note 8, at 54–55.
[24] *Supra* note 8, at 59–60.

consequential interpretive challenges in contemporary Indian insurance law. This paper has analysed that, on a purposive and textually faithful reading, the definitional categories of fraud, dishonesty, and forgery under standard Fidelity Guarantee Insurance policies are capable of encompassing cybercrime perpetrated by employees. The Information Technology Act, 2000 provides a statutory framework that aligns with and reinforces this interpretation, characterising employee cybercrime as a legally actionable wrong that results in direct pecuniary loss the core elements of a fidelity claim.

However, this inclusivity is qualified. Discovery period limitations, the absence of explicit digital asset coverage, outdated additional warranty conditions, and the demanding evidentiary requirements for cybercrime claims create conditions of practical uncertainty that disadvantage insured employers. These gaps cannot be resolved solely through judicial interpretation, they require affirmative regulatory intervention by IRDAI in the form of updated standard policy terms and the mandatory integration of cyber-specific endorsements within fidelity products.

The global trajectory of cyber insurance towards the convergence of fidelity and cyber risk within integrated insurance frameworks, and towards the insurance industry functioning as a de facto cybersecurity regulator provides a ready model for Indian regulatory reform. The employer who entrusts an employee with access to digital systems stands in precisely the position that the law of fidelity insurance has always recognized i.e., one who has extended trust and who is entitled to protection when that trust is abused, whatever the medium through which the abuse occurs.