IN THE HIGH COURT OF FIJI AT SUVA
CIVIL JURISDICTION

Civil Action No. HBC 381 of 2019

BETWEEN : **HANSONS INVESTMENTS (FIJI) PTE LIMITED** a limited Liability company having its registered office at 8 Miles, Nasinu, Fiji.

1ST PLAINTIFF

AND : **HANSONS (NABUA) HOLDINGS PTE LIMITED** a limited liability company having its registered office at 8 Miles, Nasinu, Fiji.

2ND PLAINTIFF

AND : **STELVIN ANIT LAL** of Makoi, Taxi Driver.

1ST DEFENDANT

AND : **RANEEL LAL** of Lot 9, Vatuwaqa, Suva, Fiji, Supermarket worker.

2ND DEFENDANT

AND : **SHALINI SHARMILA NAIDU** of Tovata, Makoi, Nasinu, Cashier.

3RD DEFENDANT

AND : **ACHAL PRASAD** of 36 Dhanji Street, Samabula, Suva, Salesgirl

4TH DEFENDANT

AND : **ARISHMA KIRAN** of Vuci Road, Nausori, Cashier

5TH DEFENDANT

AND : **KARISHMA MAHARAJ** of Narere, Nasinu, Fiji, Manager.

6TH DEFENDANT

AND : **SWASTIKA NIKATNI NAND** of 9 Miles, Nakasi, Occupation Unknown.

7TH DEFENDANT

AND : **SOFIA FAMEEZA GAZNABI** of Lot 15, Mana Street, Narere, Cashier.

8TH DEFENDANT

AND : **SNEH SHERIN MALA** of 9 Miles, Nakasi, Fiji, Manager.

9TH DEFENDANT

Counsel: Ms Somathi K and Ms Kumar M for the Plaintiffs

First Defendant appeared in person

For 3rd Defendant Mr Chand P

For 4th,5th ,6th and 8th Defendants Mr. Chand A

For 9th the Defendant Mr. Gosai S

Date of Judgment: 18.11.2025

JUDGMENT

INTRODUCTION

[1] The Plaintiffs operate two Total service stations (Makoi and Nabua) and claim the nine Defendants, former employees working as cashiers and managers between 2017-2019, embezzled or misappropriated sums stated against each defendant, through systematic shot fall during their shifts. The shortfall of revenue for the two service stations triggered a series of investigations or forensic audits of the Point of Sales (POS) system called Infinity (Infinity). According to Plaintiffs Defendants were able to use various methods to take money without being shown in system reconciliation and D/L reports.

FACTS

[2] According to the submissions of Plaintiff between 2017 and 2019 the defendant cashiers (and two managers who also worked cashier shifts) embezzled money from the Makoi and Nabua Total service stations by exploiting specific methods to in the Infinity POS system:

a. Mid-shift User ID switching (logging in as another cashier so those sales were excluded from the shift's DL/Financial Report).
b. Printing the DL Report early (before shift end) so later cash sales were not captured.
c. Disconnection of the POS for a while some transactions are done and reconnection , so that those entries are not shown in D/L or reconciliations
d. Colluding with the duty manager to sign off a false (understated) DL Report + manual Balance Sheet while the true sales (visible only in the back-end Excel extract) were much higher.

[3] The difference between the true sales was produced through Excel Summaries or Extracts where itemized sales were captured with time and sale price. This is not a system generated document where Plaintiffs allegedly converted system generated data from one medium in to Excel Extracts.

[4] Plaintiffs at all material times used a widely used software in Fiji "Infinity" which was supplied by Total . Some Defendants had prior experience with system and used in other shops in Fiji and had not experienced any issue with the system.

[5] Plaintiffs produced system generated documents relating to D/L Reports and Balance Sheets and Reconciliation along with Defendants' handwritten Balce Sheet for each shift in question. According to these there were no discrepancies, and the false DL Report/Balance Sheet figure is the amount stolen in each instance stolen.

PLAINTIFF'S EVIDENCE

[6] Three witnesses Mohitesh Kant was in charge of overview of operations and discovery of shortfall of money via cash-flow crisis in late 2019. The internal auditing team conducted a forensic audit to detect embezzlement of money by the Defendants .Neha Mani (PW2) and Ms. Maemoon Nisha (PW3) who assisted investigation gave evidence at hearing.

[7] They took court through every impugned shift, batch by batch, using the Excel summaries, DL Reports, Balance Sheets and transaction lists, proving the amount not paid by Defendants on each occasion.

DEFENCE EVIDENCE

[8] The four defendants who gave evidence (1st, 4th, 6th and 8th) all denied allegation

[9] Their evidence was contradictory on critical points (how long it takes to log out/in with another User ID, whether managers knew cashiers' PINs, etc.) and did not undermine the documentary evidence.

RELIEF SOUGHT

[10] Judgment against the defendants (jointly and severally were appropriate) for the full amounts allegedly embezzled as stated below, and the interest.

DEFENDANT	TOTAL MONIES MISAPPROPRIATED
Stelvin Anit Lal	$ 4, 488.09
Shalini Sharmila Naidu	$ 11, 597.48
Achal Prasad	$ 10, 589.21
Arishma Kiran	$ 7, 222.57
Karishma Maharaj	$ 32, 245.98

Sofia Farmeeza Gaznabi	$ 20, 388.61
Sneh Sherin Mala	$136, 805.79
TOTAL	**$223, 337.70**

[11] Plaintiffs submit documentary evidence is proved the methodology utilized by Defendants.

[12] The core of the proof is reliant on 'Excel Extracts' of each shift where cash shortfall is alleged. This is not a system generated document but allegedly an extract of system generated electronic evidence transformed into an Excel Sheet. Witnesses for the Plaintiff could not state more on the said Excel Summaries.

[13] It should be borne in mind without this Excel Summaries other documents which were system generated do not show alleged discrepancy in money collected and deposited in safe.

[14] Both Submissions for the Defendants disputed evidence submitted. In a nutshell their submissions are based on the Civil Evidence Act 2002. Section 18 of the Electronic Transactions Act 2008 is not dealt with in written submissions filed by Plaintiff and Defendants.

CAUSE OF ACTION

[15] Plaintiffs allege the money was stolen, misappropriated or in simply they were not properly accounted by Defendants.

[16] All the Defendants worked at relevant times as employees of Plaintiffs, and they were entrusted with sales at their respective service stations.

[17] So simply the Plaintiffs' claim relates to restitution or money had and received according to paragraph nine of the statement of claim.

[18] In NZ High Court decision of *Torbay Holdings Ltd v Napier* [2015] NZHC 2477; BC201563341 discussed the claim relating to money had and received in following manner;

> **"Money had and received**
>
> **[163]** The second cause of action alleges that Mr and Mrs. Napier have had and received money, being the total sum of the salary overpayments and the unauthorized payments. The statement of claim alleges that the total sum of the salary overpayments and the unauthorized payments belonged to Torbay Holdings and Torbay Rest Home and is owed by Mr and Mrs. Napier to them.
> **[164]** A claim for monies had and received is a personal restitutionary remedy based on the concept of unjust enrichment.[1] It requires only receipt of money by a defendant who has no right to retain it or who has improperly disposed of it. The claim does not depend on proof of

[1] *Worldtel NZ Ltd v Kim* HC Auckland CIV-2009-404-001158, 30 September 2011 at [27].

any wrongdoing or impropriety on the part of the recipient,[2] or on ongoing retention of the money or its value.[3] The cause of action is complete when the money is received. Although based in the doctrine of unjust enrichment, the claim is not the same as a cause of action for unjust enrichment. Unjust enrichment is simply a term for the underpinning doctrine of law behind various restitutionary remedies.[4]

[165] For example, in *General Distributors Ltd v Hilliard*, [5] an employee who defrauded approximately $400,000 from her employer through manipulating accounting procedures, banking arrangements and the provision of fictitious refunds was found liable in a summary judgment application for monies had and received. The Court found she had no defence to the claim. It was not her money.

[166] As noted above, a claim for money had and received does not depend on proof of any wrongdoing or fault on the part of the recipient. However, the underpinning of the claim for money had and received in unjust enrichment consequently requires some element of unjustness in the defendant retaining the money he had received. This has been highlighted in other cases:[6]

An action for money had and received is based on the receipt of money by a defendant who **no longer has the right to retain it or has improperly disposed of it**. Other than that, the claim does not depend on proof of any wrongdoing or fault on the part of the recipient.

[167] This dictum recognizes that the action for money had and received is not a claim based on the personal conscience of the recipient. Instead, the unjust assessment is focused on determining whether the retention of the money would unjustly enrich the defendant, who has no real right to the money. To this extent, the claim is complete when the money is received, if retaining the money would be unjust, as the defendant has no right to retain it. Heath J, in a recent case, saw some element of unconscionability or unjustness as being a key requirement to make out money had and received claims.[7] This recognizes the underlying focus of money had and received claims, in unjust enrichment."

[19] Accordingly, Plaintiff has to prove that Defendants had received the money but failed to pay them in full . For this Plaintiff used documentary evidence including handwritten balance sheet provided by respective cashier at the end of their shifts and Infinity System generated evidence and also Excel Summaries or Extracts.

[20] According to Plaintiffs documents Defendants had prepare a balance sheet for each shift and money in terms of that were deposited in the safe before they change over to next person. This handwritten balance sheet tallied with other Infinity system generated documents such as D/I reports and reconciliations, but

---

[2] *Agip (Africa) Ltd v Jackson* [1990] Ch 265 ; [1989] 3 WLR 1367 at 1380.

[3] *Martin v Pont* [1993] 3 NZLR 25 at 30.

[4] Lord Goff and Gareth Jones *Goff & Jones The Law of Restitution* (7th edition, Sweet & Maxwell, London, 2007) at [1-013].

[5] *General Distributors Ltd v Hilliard* HC Auckland CIV-2008-404-1057, 16 March 2009.

[6] *Nimmo v Westpac Banking Corporation* [1993] 3 NZLR 281 (HC) at 238.

[7] *Levin v Ikiua* HC Auckland CIV-2007-404-6810, 24 July 2009 at [92].

according to Plaintiffs such reports did not depict true or actual sales, and they were under reported using various methods.

[21] Central to Plaintiffs' claims against all the defendants are Excel Summaries or Excel Extracts which according to Plaintiffs show individual sales during shifts and these Excel Summaries show more sales than what Defendants prepared and also system generated documents.

Admissibility of Electronic Evidence in Civil Action

[22] Section 18 of Electronic Transactions Act 2008 states,

> "**18** **(1)** Notwithstanding the provisions contained in the Civil Evidence Act 2002 or any other written law, the following provisions shall apply to Parts 2, 3 and 4 of this Act, in any civil proceedings.
>
> **(2)** Any information contained in a data message, electronic document, electronic record or electronic communication-
>
> a) Touching any fact in issue or relevant fact; and
> b) Complied, received or obtained during the course of any business, trade or profession or other regularly conducted activity,
>
> Shall be admissible in a civil proceeding under this Act, provided that direct oral evidence of such fact in issue or relevant matter, if available shall be admissible; and there is no reason to believe that the information contained in a data message, electronic document, electronic record or any electronic communication is unreliable or inaccurate.
>
> **(3)** The courts shall, unless the contrary is proved, presume the truth of information contained in a data message electronic document, electronic record or electronic communication made by a person or government entity, that the said data message, electronic record or electronic communication was made by the person who purported to have made it and similarly, shall presume the validity of any electronic signature or authentication method or distinctive identification."

[23] The digital transformation of commercial transactions has fundamentally altered the evidentiary landscape in forensic auditing. Where once the forensic auditor traced paper trails through physical ledgers and correspondence, today's investigation traverse server logs, database entries, encrypted communications, and algorithmically generated records. This paradigm shift presents a profound challenge to legal systems historically anchored in the tangible and immutable nature of documentary evidence.

[24] Section 18 of Electronic Transactions Act 2008 (ETA 2008) represents the legislative response to this challenge, establishing foundational principles for the

admissibility and evidential weight of electronic records. Drawing heavily from the UNCITRAL Model Law on Electronic Commerce (1996)[8], this provision embodies a critical policy objective: to create functional equivalence between electronic and paper-based evidence while maintaining rigorous standards of authenticity and integrity.(See Gap analysis of cyberlaws in Pacific Small Island Developing States[9]

[25] Section 18 of ETA 2008 is significantly different from the original provision which was fully repealed in 2017, and legislative history of the said provision also shows the legislative intent, which qualified presumption of electronic evidence to business activities or such regularly conducted 'activity'.

A. Legislative Architecture and Policy Objectives

[26] Section 18 of the ETA 2008 establishes three interlocking principles that govern the admissibility of electronic evidence. First, the provision enshrines the "principle of non-discrimination", mandating that courts must not deny admissibility to a data message merely on the grounds that it constitutes electronic rather than physical evidence. This directly implements Article 5 of the UNCITRAL Model Law, which declares that "*Information shall not be denied legal effect, validity or enforceability solely on the grounds that it is not contained in the data message purporting to give rise to such legal effect, but is merely referred to in that data message*[10]

[27] Second, Section 18 operationalizes the "best evidence principle" in the digital context when such evidence qualified certain conditions. It provides that even where a data message is not in its original form, it remains admissible if it represents the best evidence that the proponent could reasonably be expected to obtain. This provision acknowledges the practical reality that electronic evidence, by its nature, exists as copies and iterations rather than unique originals, and that insistence on "originals" in the traditional sense would render electronic evidence perpetually inadmissible. It is important in such instance to lead evidence of relevant persons who accessed or copied such evidence to provide evidence as to authenticity of such electronic evidence .

[28] Third, the provision mandates that courts must give "due evidential weight" to data messages, with such weight assessed according to four specified criteria: (1) the reliability of the manner in which the data message was generated, stored or communicated; (2) the reliability of the manner in which its integrity was maintained; (3) the manner in which its originator was identified; and (4) any other relevant factors. These criteria establish a functional equivalence framework that identifies the essential qualities of reliable evidence regardless of medium.

---

[8] https://unctad.org/system/files/official-document/dtlecde2024d6_en.pdf

[9] This study is part of the Pacific Digital Economy Programme, a joint effort with the United Nations Capital Development Fund and the United Nations Development Programme. This initiative builds on long-standing assistance from UNCTAD to the Pacific Island Forum Secretariat and its members in support of the development of e-commerce, especially in the conduct of eTrade Readiness Assessments and E-commerce Strategies in the region. https://unctad.org/publication/gap-analysis-cyberlaws-pacific-small-island-developing-states

[10] https://uncitral.un.org/sites/uncitral.un.org/files/media-documents/uncitral/en/19-04970_ebook.pdf

B. The Technology-Neutral Philosophy

[29] UNCITRAL inspired approach, as embodied in Section 18 of ETA 2008 lies in its technological neutrality. The provision does not prescribe specific software, hardware, or cryptographic algorithms. Rather, it articulates the legal outcomes that must be achieved reliability, integrity, and attribution while remaining agnostic as to the technological means by which these outcomes are secured. This creates a flexible framework capable of accommodating technological evolution, from magnetic tape storage systems in the 1990s to contemporary cloud-based distributed ledger technologies.

[30] However, this neutrality comes with a burden: the proponent of electronic evidence must affirmatively demonstrate that the chosen technological methods achieve the stipulated legal outcomes. The statute provides the gateway; the party seeking admission must prove certain conditions . This is relevant in this action as the vital piece of evidence Excell Summaries or Extract were documents prepared by forensic auditing. They were documents prepared in the investigation and allegedly show all sales during a shift.

[31] So, the alleged shortfall of cash is shown by comparison of these Excel Summaries with Balance Sheet of Plaintiff prepared. The short fall was detected years after the alleged leakage of money at the hands of the Defendants. These were not Infinity System generated documents and were produced using data allegedly extracted from Infinity System. The witnesses could not state details of this process as they had played only a supporting role in the forensic audit.

The Admissibility of System-Generated Electronic Evidence in Forensic Auditing: An Analysis of Section 18 of Fiji's Electronic Transactions Act 2008

[32] Digital Forensics and what are techniques and tools used discussed in Sixth Australian Digital Forensics Conference,[11] by presentation 'Digital forensics and the legal system: A dilemma of our times'[12] states,

> "Biros and Weiser (2006) define digital forensics as "**scientific knowledge and methods applied to the identification, collection, preservation, examination, and analysis of information stored or transmitted in binary form in a manner acceptable for application in legal matters"**. Digital forensic investigation requires defined procedures that comply with industry practice, organizational practice and appropriate laws, whether as part of a criminal investigation or as part of a more general security incident response. The technique and tools used by forensic investigators may vary,

[11] Edith Cowan University, Perth Western Australia, December 3rd 2008.
This Conference Proceeding is posted at Research Online as part of computer science commons https://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1040&context=adf(18.11.2025)

[12] by James Tetteh Ami-Narh Edith Cowan University taminarh@student.ecu.edu.au Patricia A H Williams Edith Cowan University, trish.williams@ecu.edu.au

however the process generally includes planning, acquisition, preservation, analysis and reporting”(footnotes deleted , Emphasis added)

[33] Alleged extraction of data relating to all the sales in a shift were generated from Infinity System using a form of forensic tool as the leakage of money were investigated two years after the alleged incident. So, all the sales relating to shifts were generated from a stored database and this evidence was analysed with Balance Sheet prepared at each shift by Defendants. This was a digital forensic investigation.

III. The Critical Limitation: The "Ordinary Course of Business" Doctrine

[34] While Section 18 of ETA 2008 establishes a rebuttable presumption regarding the authenticity of electronic documents generated by information systems, this presumption is explicitly conditioned on the evidence being produced "in the ordinary course of business." This seemingly innocuous qualifier has profound implications for forensic audit evidence.

[35] Even a routine internal audit can be considered as an ordinary course of business depending on the manner it was conducted, but when specific investigation or forensic audit is conducted such evidence cannot be considered as ordinary business

[36] The reports generated or transformed to another medium should be proved by the party relying on Excel Summaries as to their authenticity and reliability. Such records or documents are admissible provided the evidence is led to the authenticity of such records. In this action witnesses could not state how the evidence or databases were accessed and whether they were securely kept . Such evidence needed to be given by information technology experts or forensic experts in information technology as to the reliability of the database they accessed and the manner in which such data was transferred to another electronic medium till they were presented to the court.

[37] The "ordinary course of business" concept derives from the common law business records exception to the hearsay rule, which permits the admission of routine business records on the theory that their systematic creation as part of regular organizational processes provides inherent indicia of reliability.

[38] Evidence generated specifically for investigative purposes falls outside the protective ambit of Section 18 of ETA 2008 from its presumption. Such evidence is not generated in the "ordinary course" of the original system's business purpose but rather represents a deliberate, investigative intervention into that system.

[39] Such evidence can be produced provided in the digital medium provided there is evidence as to reliability and there was no reason to believe such evidence is unreliable. The evidence produced through Excell Extracts is far from that as they were transferred from a different medium, but the witnesses were unable to state how such transfer was done and or who did it and as to accuracy of such transfer.

B. THE FOUR-FACTOR AUTHENTICATION TEST

[40] Four reliability criteria provide the framework through which common law courts assess electronic evidence authenticity. Research article published on 12.9.2025 on 'The admissibility of digital evidence from open-source forensic tools: Development of a framework for legal acceptance'[13] stated,

> "Digital forensics has become an essential discipline that deals with methodologies, techniques, and tools used in the identification, collection, preservation, and analysis of digital evidence for legal purposes. The field has expanded to address eight primary focus areas: basic theory and methods, physical equipment and forensic methods, image forgery identification, file recovery and data extraction, smartphone and social network forensics, case-based forensics, automatic identification technology, and cloud forensics. This multifaceted approach enables investigators to deal with different kinds of digital crimes, as well as to preserve evidence quality throughout the investigation lifecycle. The "Forensic of Things" paradigm that is emerging extends these capabilities to IoT environments because traditional forensic approaches are not sufficient in IoT due to device diversity, proprietary communication protocols, and data volume challenges].
>
> **Digital forensic procedures follow a standardized process to guarantee that the evidence is admissible**. This process starts with the **identification of potential digital evidence sources, followed by the preservation of the digital crime scene, collection by forensically sound methods, examination while maintaining the chain of custody, analysis to determine relevance, and presentation in court-admissible formats**. Each stage **must adhere to strict protocols to avoid evidence modification or loss, which may render the findings inadmissible in legal proceedings**. The methodological rigor of these procedures, as observed in the study by Edward et al., affects judicial acceptance of digital evidence, thereby emphasizing the essential connection between technical processes and legal requirements.
>
> Digital evidence is a vital element in cybercrime prosecutions, because it includes digital information that has probative value in legal proceedings. **Such evidence is admissible if it can be proven authentic, reliable, complete, and in a good chain of custody**. Current developments in different jurisdictions show a growing trend to standardize the retrieval and protection of digitally stored information to enhance legal validity. This trend is a manifestation of the fact that digital evidence has its own set of problems that are different from physical evidence, thus necessitating specialized

[13] : Ismail I, Zainol Ariffin KA (2025) The admissibility of digital evidence from open-source forensic tools: Development of a framework for legal acceptance. PLoS One 20(9): e0331683. https://doi.org/10.1371/journal.pone.0331683
https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0331683(18.11.2025)

measures to ensure that it is not compromised during the investigative process.

The use of international standards is important for the development of uniformity in handling digital evidence. The ISO/IEC 27037:2012 standard provides detailed guidance for the identification, collection, acquisition, and preservation of digital evidence, whereas the ISO 27050 series address electronic discovery processes]. These standards provide a comprehensive description of the entire lifecycle of digital evidence management, from identification to preservation, analysis, and presentation. A comparison of these standards shows that there are complementary approaches that result in the development of effective frameworks for the admissibility of digital evidence across jurisdictions when properly integrated. The reason for standardization is even more significant in light of the fact that cybercrime has no borders, and investigations and prosecutions often require cross-jurisdictional collaboration." (Foot notes delete and emphasis added)

[41] Plaintiffs are commercial establishments with their service stations under multinational energy brand . When it had used a POS system such as Infinity it is also important to follow some internationally accepted standards such as ISO/IEC 27037:2012 which is an international standard titled "Information technology - Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence"*.It provides practical guidance for first responders, digital forensic experts, and investigators on handling potential digital evidence (e.g., from computers, mobile devices, networks, or cloud storage) in a forensically sound manner. There is no evidence that Plaintiffs used such standards in their ICT plan or more specifically relating to Infinity software, or in forensic audit.

[42] The main goal of such standards is to ensure evidence remains "authentic, reliable, and admissible" in legal or disciplinary proceedings by preventing contamination or alteration.

[43] Key focus areas are the following:

a. Identifying sources of digital evidence

b. Safe collection and acquisition (e.g., using write-blockers, creating forensic images)

c. Proper preservation and storage

d. Documentation and maintaining a chain of custody

[44] It is part of the ISO/IEC 27000 standards but focuses specifically on the initial handling phases of digital forensics rather than full forensic analysis or incident response frameworks covered in other standards like ISO 27035 or 27041-27043.

1. Reliability of Generation, Storage, and Communication

[45] There was no evidence before the court as to how the information generated for Excel Extracts was stored or they were secure. There was no evidence as to method of transferring such data into Excel Extracts and

[46] There is no issue as to the reliability of the Infinity system in its business application or generation of usual reports, but this is not sufficient for the reliability of Excel Summaries as they were generated in investigation. So, reliability will heavily be dependent on the manner of storage and management of such database for long terms such as two years and who had access to such data and what tools or medium used for generation of relevant data from storage and method of communication used. There is no evidence on these vital issues as the witnesses called by Plaintiffs were not directly involved in the audit or able to give evidence of these vital issues.

2. Reliability of Integrity Maintenance

[47] This factor has emerged as the critical battleground in forensic evidence admissibility. The question is not merely whether the original system was reliable, but whether the evidence, as ultimately presented to the court, has been maintained in an unaltered state throughout the investigation. In this case there is no evidence of such reliability.

3. Manner of Originator Identification

[48] The third factor concerns attribution establishing that the evidence originated from the claimed source. In this action Plaintiffs' own Infinity System is used so there is no issue as to origin as it comes from its own system and not from third party extracted data, but there was no evidence as to reliability of archived data used to generate all POS recordings, in Excel Summons.

4. Other Relevant Factors

[49] Courts have interpreted this catch-all provision broadly, considering factors such as the existence of audit trails, access controls, employee training protocols, and the temporal proximity of the evidence to the events in question.

[50] Section 18 of Fiji's Electronic Transactions Act 2008 establishes a progressive, technology-neutral framework for the admissibility of electronic evidence, grounded in the internationally recognized UNCITRAL principles of non-discrimination, functional equivalence, and reliability assessment. However, the provision's "ordinary course of business" limitation excludes from automatic presumption the very category of evidence most critical to forensic auditing: investigative generated electronic records.

[51] For such evidence, admissibility is not granted by statutory fiat but must be earned through adherence to forensic best practices validated by common law

jurisprudence. The four-factor reliability test mandated by Section 18 finds practical expression in the requirement for forensically sound acquisition methods, cryptographic hash verification, secure chain of custody protocols, and expert testimony capable of explaining these technical safeguards in legally cognizable terms.

[52] In the digital age, the forensic auditor must be not only an investigator of financial irregularities but also a guardian of electronic evidence integrity, a translator between technological and legal domains, and a builder of unassailable evidential foundations. Through this multifaceted role system-generated electronic evidence transcends its inherent volatility to achieve the status of reliable, admissible, and ultimately persuasive proof in the pursuit of justice.

[53] In this action Defendants who worked in respective service stations as cashiers had prepared a balance sheet for the respective shifts and these were reconsolidated from the system generated reports at that time, so that there was no shortfall of money.

[54] Alleged methods used by Defendants were discovered when individual sales during the shifts were verified with the reports generated by Infinity system. So pivotal document in the proof of Plaintiffs' case are Excel Summaries or extracts. These were not system generated documents. These were allegedly extracted from a database . So firstly, there was no evidence of reliability or security as to said database as it was accessed years after the alleged incident.

[55] The witnesses called by Plaintiffs could not provide evidence as to manner in which electronic evidence was obtained as they only assisted in tasks such as photocopying and were not directly involved in extraction of such electronic evidence.

[56] Apart from that it was evidenced that the electronic evidence produced by the system was converted into Excel sheets and there was no evidence as to reliability of such transfer as they should be error free.

[57] There was no evidence as to preservation of such evidence before production at hearing serious issues as to reliability of Excel summaries which were not system generated document and lacked any form of authentication in such records as opposed to system generated documents.

[58] In the circumstances it is unreliable to base allegations against Defendants on Excel Summaries or extracts .

[59] On this basis action is dismissed against all defendants.

[60] There is a counter claim filed by eighth Defendant, I do not need to consider counter claim as the action against the nineth Defendant is dismissed on a preliminary issue. Accordingly, the counter claim is also dismissed without cost.

CONCLUSION

[61] The Plaintiff had relied on the evidence of electronic evidence obtained from forensic audit but was unable to prove the authenticity of Excel Summaries . This was due to witnesses were unable to state the details of such forensic audit as their involvement was only supportive and lacked expertise in forensic audit. Next there were no evidence to show how data in Excel Summaries were extracted and then transferred to Excel Summaries without compromising the authenticity and reliability. Then how such evidence was authenticated not proved. Finally there was no evidence as to chain of custody as to such evidence. So Excel Summaries cannot be relied by court.

[62] Without Excel Summaries Plaintiffs ' claims against all the Defendants cannot be proved on balance of probability. Plaintiffs claim against all the defendants are struck off. Counter claim of eight Defendant is also struck off. Nor cost ordered considering the circumstances.

FINAL ORDERS;

1. Statement of Claim against all the Defendants struck off.

2. The counter claim of the eighth Defendant is struck off.

3. Parties to bear the costs.

HIGH COURT OF FIJI SUVA

.....

Deepthi Amaratunga

Judge

At Suva this 18th day of November, 2025.

Solicitors

Shelvin Singh Lawyers

Amrit Chand Lawyers

Sunil Gosaiy Law Firm