An Anatomy of Bank Fraud

Janek Ratnatunga

Abstract

The philosophy of Sun Tzu highlights that even the most fortified systems can be compromised by minor oversights. In today's context, such negligence often manifests as an employee inadvertently clicking a phishing link. This vulnerability was starkly exposed in the case of the *National Development Bank PLC* heist in Sri Lanka, where insiders exploited an overlooked point to orchestrate one of the country's most significant bank frauds, amounting to approximately Rs. 13.2 billion (AUD 66 million). This article dissects the fraud's anatomy from a management accounting perspective, touching on aspects like governance, audit roles, KYC, money laundering, cryptocurrencies, and the significance of clear financial statements.

The fraud was centred on the CEFT Suspense Accounts, which should normally show temporary balances, but instead showed a massive, unexplained increase. The internal audit process failed to flag the unusual increase in accounts receivable balances, while external auditor Ernst & Young did not identify it as a material anomaly. Similarly, the Board Audit Committee did not detect the growing risk, pointing to broader governance and procedural failures.

The article argues for simplified and digital financial reporting to enhance transparency and facilitate easier detection of anomalies. By presenting financial statements in accessible formats like Excel and using digital tools, stakeholders could more effectively monitor financial health and prevent future occurrences of fraud.

Introduction

In ancient warfare, walls were built to keep the enemy out. In the digital age, the enemy is already inside the walls, testing thousands of digital doors every second.

Cybersecurity is no longer an IT nuisance; it is a paramount strategic concern. This reality reflects the core philosophy of *Sun Tzu's The Art of War*, which emphasises that the most fortified city is often conquered not by a grand, visible siege, but by a single point of negligence at an overlooked side entrance (Sun Tzu 2003). It implies that even the most fortified systems are vulnerable not to the obvious, but to a moment of negligence at an overlooked point of entry. In the modern context, that unguarded gate is often a single employee clicking on a phishing link.

This "overlooked point of entry" was used by knowledgeable insiders to carry out one of the largest frauds to date in the Sri Lanka banking system, the *National Development Bank PLC* heist, amounting to approximately ***Sri Lankan Rupees 13.2 billion (AUD 66 million).***

This article looks at the anatomy of this bank fraud from a management accounting perspective, as it covers many areas that are covered in the CMA programme such as *enterprise governance, the role of boards and audit committees, KYC, money laundering, cryptocurrencies, forensic audits, whistleblowing* and the need for *simple audited financial statements.*

The Reported Facts

Let us first examine the facts as reported in the regulatory documentation, stock market announcements, and audited financial statements. Then, we will consider the speculations that have arisen as a result.

There Were Two Frauds

The first smaller fraud was detected on November 27, 2025, where the suspects were accused of misappropriating **Rs. 290 million** from the bank's general ledger account. NDB had lodged a formal complaint with the *Financial Crimes Investigation Division (FCID)* of the CID; but made no disclosure to the *Colombo Stock Exchange (CSE)* about the CID investigation that resulted from this complaint.

The second larger fraud came to light when the *Central Bank of Sri Lanka* (CBSL) issued a *regulatory statement* on April 6, 2026, stating that NDB had uncovered an internal fraud that could lead to a significant loss being incurred. The preliminary estimate was approximately **Rs. 380 million**. The NDB informed CBSL that no customer accounts or deposits have been affected by this fraud.

Preventing a Run on the Bank

CBSL reassured the public that it had carried out a preliminary assessment of the financial impact on the basis of the information provided by NDB and was satisfied that notwithstanding the reported loss, the prudential ratios relating to capital adequacy and liquidity continued to be at levels above the *minimum regulatory requirements.* CBSL also said that in the event of necessity, NDB will be able to access *temporary liquidity* available from CBSL to banks under the provisions of the relevant laws and schemes already in place.

On the same day that the CBSL issued the above *regulatory statement* (April 6) *the Colombo Stock Exchange (CSE)* imposed a *trading halt* on NDB shares following the bank's follow-up disclosure that the estimated losses of the second fraud had grown to approximately **Rs.13.2 billion.**

The Common Electronic Fund Transfer (CEFT) system

The indication was that this massive fraud involved the *Common Electronic Fund Transfer (CEFT) system,* which is Sri Lanka's real-time electronic interbank fund transfer mechanism for retail transactions. Note that it is probably more difficult to manipulate the *Real Time Gross Settlement (RTGS) system* than the *CEFT system.* The primary difference between RTGS and CEFT payments lies in their intended transaction value, settlement speed, and operational mechanics. RTGS is designed for high-value, instant, one-to-one settlements, while CEFTS is designed for lower-value, instant, 24/7 retail transactions.

Accounts Receivable Balances

Anyone examining NDB's *Audited Financial Statements* could have seen (if they looked closely) that the historical *'Common Electronic Funds Transfer (CEFT)'* ***Accounts Receivable*** balances at NDB had been stable at around Rs. 1.4 billion to Rs. 1.9 billion between 2021 and 2023. However, by the end of 2024, these balances had risen to **Rs. 3.1 billion.** Then, by the end of 2025, the CEFT receivable balance had surged to **Rs. 12.22 billion**. *This was a fourfold increase in just one year.*

Thus, an (after-the-fact) question can be raised as to why, despite appearing in the bank's own audited financial statements, this massive spike was not flagged for more detailed verification by internal auditors, external auditors, or the board's audit committee.

On April 10, 2026, as a result of this fraud, *Fitch* downgraded NDB's Rating from A (lka) to 'A-(lka)'and said the outlook was negative (Fitch, 2026)

The Speculations

Reports in the regular news media (see Chandrasekera, 2026) have stuck, by and large, to the reported facts as outlined above. However, *social media* has run amok, often with wild speculations with names of non-existent villains and heroes. However, some reports published on social media have displayed traits of very good investigative journalism by sticking as much as possible to the facts and not naming the key alleged perpetrators who are still to be brought to justice at the time of writing (see Kushan, 2026).

Some of the more credible speculations on social media, and also the results of the author's own investigations with very senior auditors, bankers and CMAs from the banking sector in Sri Lanka, are discussed in this article. There have been *CMA Workshop* participants from almost all banks in Sri Lanka, as well as the Central Bank; and the fact that the author was in Sri Lanka when the second fraud was exposed enabled him to have direct conversations with many such individuals.

Unauthorised Transactions

There now is very credible speculation that over the period 2024 to early 2026, the primary suspect, an internal operations manager, gained access to *the login credentials of two other officers* to enter the system and authorise CEFT transactions that moved funds out of NDB's internal accounts. This effectively defeated the segregation of duties controls. In a properly functioning system, no single individual should be able to both initiate and authorise a transaction. By using others' passwords, the primary suspect created the appearance that multiple authorised persons had approved the transactions.

The unauthorised transactions were mostly carried out on the *weekends* when oversight was weaker, staffing was reduced, and real-time human monitoring was less active. This timing also delayed reconciliation, giving the perpetrators time to cover their tracks before the next business day.

The fraud was centred around NDB's *Department of Payments and Settlements*. This unit handles all electronic fund transfers and interbank settlements. The alleged primary suspect held a senior position within this department. This gave him direct access to the systems used to process CEFT transactions.

There is strong speculation that this second and bigger fraud is related to the first smaller fraud either because they were carried out by perpetrators known to each other or that the first fraud opened doors or showed weaknesses in the internal controls related to CEFT transactions.

The Key Account Targeted.

The key target was the ***CEFT Suspense Accounts***. These accounts are used to track funds in transit between banks. Under normal operations, these suspense accounts should have temporary balances that are cleared during regular reconciliation.

In the *NDB Chart of Accounts*, the CEFT suspense accounts sit within ***Other Financial Assets*** *which include Receivables arising from CEFT transactions.* Thus, if the balances in the CEFT suspense accounts increase, this will increase the *Accounts Receivable* balances.

The Scheme

The scheme involved creating unauthorised CEFT transactions that moved funds out of NDB's internal accounts.

This was **not a sophisticated scheme**. For example, in the normal course of bank business, the payment of rent for (say) and owner of a building housing an NDB Bank's branch location would be recorded as *Dr. Rent; Cr. Cash*. However, in this case, the fraudulent transaction was most likely recorded as *Dr. Suspense Account; Cr. Cash.* The cash was electronically transmitted to an account in another bank under the control of the perpetrator(s).

In a trading firm, a reduction of a company's cash by Rs 13.2 billion would certainly not go unnoticed, but in a bank, where customers are constantly depositing and withdrawing cash, the cash balances were well within that expected in normal operations and thus did not trigger alarm bells.

In the *NDB Chart of Accounts*, the CEFT suspense accounts sit within ***Other Financial Assets,*** *which include Receivables arising from CEFT transactions.* Thus, if the balances in the CEFT suspense accounts increase, this will also increase the overall *Accounts Receivable* balances.

Thus, anyone examining the ***NDB*** **Audited Financial Statements** could have seen (if they looked closely) that the historical *'Common Electronic Funds Transfer (CEFT)'* ***Accounts Receivable*** balances at NDB whilst being stable at around Rs. 1.4 billion to Rs. 1.9 billion between 2021 and 2023, had risen to **Rs. 3.1 billion** by 2024. By the end of 2025, the CEFT Accounts Receivable balance had *skyrocketed* to Rs. 12.22 billion, marking a fourfold increase in just one year.

Thus, an (after-the-fact) question can be raised as to why; despite appearing in the bank's own audited financial statements, this massive spike was not flagged for more detailed verification by internal auditors, external auditors, or the board's audit committee. This issue will be discussed later.

Money Laundering

There is much speculation as to the use of multiple banks as intermediaries (layering), splitting transactions (structuring) and using the accounts of multiple people (smurfs) and converting the ill-gotten funds to cryptocurrency. This highlights the weaknesses in the AML framework of both NDB and CBSL

The transactions were structured to stay just below the *Rs. 5 million per transaction ceiling* for CEFT transfers. This was done to avoid triggering automated threshold alerts. This technique is similar to what is known as *"structuring"* or *"smurfing"* in money laundering terminology. While often used interchangeably, "structuring" is the broader tactic of splitting transactions, whereas "smurfing" specifically employs multiple people (smurfs) to make these deposits across various accounts.

These 'smurfs' were those with accounts in other banks, as there are reports indicating that CBSL visited several other banks that received funds linked to the NDB fraud. This is a classic money laundering technique known as *layering,* which obscures the origins of illicit funds There is speculation that officials in other banks were also involved in opening up legitimate accounts for these smurfs, bypassing KYC requirements.

Opening up bank accounts for unsuspecting smurfs is not difficult. One bank manager said he knew of a case where a person was chatted up at a bus stand by a bank officer and promised a credit card if she opened a bank account. The account was then opened with a legitimate name, address, ID

number, etc., for KYC purposes. The account remained under the control of the bank officer long enough for in to be used for fraudulent purposes.

There is also an allegation that Rs. 12.8 billion left the country without being flagged. If found to be true, this represents failure of *anti-money laundering (AML)* controls by both NDB's internal AML monitoring unit, and the CBSL's broader foreign exchange monitoring controls. There is speculation that a portion of the funds was also converted into *cryptocurrency*. suggesting that the perpetrators used digital currency to move and hide stolen funds. [*See Ratnatunga (2021) for a detailed analysis of money laundering in both Fiat and Crypto currencies*].

The Red Flags

Clearly there need to be questions asked of the NDB's *Governance Procedures*. This includes its *internal control processes*, its *internal audit processes*, its *external audit processes* and the oversight by its *Audit Committee*. This article will finally argue that the presentation of its *audited financial statements* prevented to a large extent from this fraud being discovered.

Failure of Internal Control Processes

Internal controls in banking are more than just a safety net; they are the fundamental framework that ensures the bank's solvency, compliance, and reputation. Because banks deal in high-volume, liquid assets (cash) and complex risks, their control environment is subject to much higher scrutiny than a typical corporation

The key areas of ***bank internal controls*** are generally categorised into five core pillars: (1) *Operational Controls & Segregation of Duties;* (2) *Credit and Lending Controls; (3) Financial and Regulatory Reporting Controls; (4) Asset and Liability Management (ALM)* and (5) *Information Technology and Cybersecurity.* The first and last pillars are particularly relevant to the NDB case,

The first pillar, ***'Operational Controls & Segregation of Duties',*** is the most visible layer of defence, designed to prevent error and fraud in day-to-day transactions. This involves:

Dual control and maker-checker systems: Requiring two people to complete every transaction. It must be initiated by one person (the maker) and independently verified and approved by a different person (the checker). This is standard practice in all well-regulated banking systems. At NDB, the maker-checker control was bypassed because the suspect used others' credentials. In a robust system, the checker would need to physically or biometrically verify their identity before approving.

Segregation of Duties: Ensuring that the person who initiates a transaction is not the same person who authorises or reconciles it. At NDB, the primary suspect defeated segregation of duties by using the passwords of two other officers. This means the system technically showed multiple authorisers, but in reality, one person controlled the entire process. Effective technology controls (such as biometric authentication or multi-factor authentication tied to individual users) would have prevented this.

Joint Custody: Physical assets (like cash and negotiable securities) are kept under the control of two or more authorised individuals.

Staff Rotation: It appears also that the bank's ***staff rotation policy was breached***. This is a fundamental banking control designed to prevent exactly this type of fraud. It appears that the same individual remained in the critical *Payments* and *Settlements* role without being rotated.

Mandatory consecutive leave periods: This policy requires employees in sensitive positions to take a continuous period of absence, during which another person performs their duties. During the leave, the employee must have *no access to any physical or virtual resources* related to their work.

The last pillar is ***'Information Technology and Cybersecurity'***. In the digital age, a bank's "vault" is its server. Unfortunately, NDB's information technology and cybersecurity controls failed at multiple levels. There was *collusion among multiple insiders* in the first fraud and most probably in the second. There was also *abuse of systems access.* The NDB suspect in the second fraud used stolen passwords.

These controls here are paramount for data integrity and include the following:

Access Controls: This category includes restricting system access based on the "Principle of Least Privilege" (only giving employees the access they absolutely need).

Audit Trails: This process requires automated logs that record every single action taken within a banking system, identifying who did what and when.

Business Continuity Planning (BCP): These are the controls and protocols to ensure banking operations can continue in the event of a cyberattack or natural disaster. [*See Singleton and Singleton (2010) for a detailed understanding of fraud auditing and forensic accounting*].

Failure of Internal Audit Processes

The internal audit process in a bank is highly structured to meet the rigorous demands of regulators. It moves from a "big picture" risk assessment down to specific testing of individual transactions. The typical lifecycle of a bank internal audit involves five steps: (*1) Risk-Based Audit Planning; (2) Engagement Planning & Scoping; (3) Fieldwork and Testing; (4) Reporting and Communication;* and (5) *Follow-Up and Monitoring.* An audit isn't closed until the gaps are plugged. This involves *Remediation Testing* to verify that the new controls are actually working and regular *Reporting to the Board.*

NDB's internal audit function failed to detect a fraud that lasted approximately 18 months. The CEFT suspense account balance grew from its historical norm of Rs. 1.4 billion to Rs. 12.22 billion. This was a clear and visible anomaly. A competent internal audit team should have flagged this discrepancy during routine reviews. The fact that it was not questioned suggests either a lack of competence, a lack of independence, or a failure of the audit scope to cover this area adequately.

Failure of the External Auditor: Ernst & Young

While Internal Audit works for the Board to improve operations, **External Audit** works for the shareholders and regulators to verify that the bank's financial health is *"true and fair".* Because banks are high-risk institutions, external audits are intensely focused on *valuation* (is the money actually there?) and *liquidity* (can the bank survive a "run"?).

The auditor starts by determining "*Materiality*"—the amount of an error that would actually matter to a shareholder. Next is the *"Evaluation of significant estimates"*. This is the most difficult part of a bank audit. Auditors don't just check math; they challenge management's *assumptions*, especially regarding (a*) Loan Loss Provisions (ECL);* and *(b) Fair Value of Derivatives.*

Then, the auditor must verify the bank's assets through independent third-party evidence, including: (a) *External Confirmations; (b) Cash Counts; and (c) Cut-off Testing to ensure that* transactions made on December 31st aren't accidentally recorded on January 1st to "window-dress" the year-end

reports. In many jurisdictions (like under ***Basel III*** *or* ***SOX***), external auditors must provide specific opinions on (a) *Capital Adequacy and (b) Anti-Money Laundering (AML).* While not always a full audit, they often test the systems that flag suspicious transactions to ensure the bank isn't violating international sanctions.

The process ends with the formal *Independent Auditor's Report*, including (a) *The Opinion; (b) Key Audit Matters (KAMs);* and the *Management Letter:* A private document sent to the Audit Committee detailing "Material Weaknesses" in the bank's systems that need to be fixed.

NDB's external auditor is ***Ernst & Young (Sri Lanka).*** E&Y audited the bank's 2025 financial statements, which reported the Rs. 12.22 billion in CEFT receivables. This was a fourfold increase from the previous year and an eightfold increase from the historical norm. We have already discussed that EY did not flag it as a material anomaly requiring deeper investigation. It is still to be determined if the private *Management Letter* sent to the Audit Committee detailed "Material Weaknesses" in the bank's CEFT systems that needed to be fixed. Given the surprise and the extent of the fraud, it is unlikely that this was flagged. *[See Ratnatunga (2016a, 2018a, 2018b, 2019) on how accounting reports only create a delusion onf the state of affairs of a company and why audit opinions are 'untrue' and 'unfair'].*

Failure of Board Audit Committee

The Audit Committee plays a critical role in the corporate governance framework, acting as a bridge between a company's board of directors, internal auditors, and external auditors. Their primary goal is to ensure the integrity of financial reporting and the robustness of internal controls.

A company is only as strong as its "checks and balances". The committee evaluates the effectiveness of the (a) *Internal Audit Function:* (b) *Internal Control Systems*; and (c) *Risk Assessment.* NDB's Board Audit Committee and the Board Risk Committee failed to identify the growing operational risk in the Payments and Settlements unit.

The Audit Committee is also responsible for establishing *Whistleblower Mechanisms* for the receipt and treatment of complaints regarding accounting or auditing matters (often called a "Whistleblower Hotline").

The strength of the whistleblower protections varies from country to country. In the USA, the *Sarbanes-Oxley Act (Section 806)* protects employees of publicly traded companies from retaliation for reporting suspected fraud. However, in *Australia***,** protections are significantly weaker (Ferguson, 2022).

Failure in Presentation of Audited Financial Statements

In the *NDB Annual Report 2025 is 556 pages long*. The financial statements only start on page 271. The *Independent Auditors Report* is on page 276,

On page 347, in ***Note 36.3*** *on* ***Other Financial Asset,*** the balance shows a fourfold surge from Rs 3.1billion in 2024 to Rs.12.2 billion in 2025. There was an *asterisk** placed against the balance stating that it was "**Other financial assets include Receivables arising from CEFT transactions"*.

Although IT systems and internal controls were listed as a *Key Audit Matter,* the auditor's concerns were satisfactorily resolved (see next). We do not know what IT systems and internal controls were specifically tested, but we do know is that the four-fold surge *in the* Accounts Receivable balances disclosed in the audited financial statements did not result in an *Audit Qualification*.

In the independent auditors report**,** '*Information Technology (IT) systems* related internal controls over financial reporting' is listed as a *'Key Audit Matter'* because: ***"****the Bank's financial reporting process is significantly reliant on multiple IT systems with automated processes and internal controls; and that key financial statement disclosures are prepared using data and reports generated by IT systems, that are compiled and formulated with the use of spreadsheets."*

However, this Key Audit Matter was resolved by the auditors by obtaining a high-level understanding of the *cybersecurity risks* affecting the bank and by testing source data of the reports used to generate disclosures for accuracy and completeness, including review of the general ledger reconciliations. We now know that the balances were reconciled using the *suspense accounts.*

The question is, *"Should this* four-fold surge *in the Accounts Receivable balances have been considered 'material" for an 'Audit Qualification'?"* After all the Banks total assets were Rs. 945 billion, which means that these *"Other financial assets'* represented ***just 1% of its assets***. This is a question for the Auditors and Audit Committee to answer.

My informed opinion is that the blame lies in *the way financial statements are presented,* and this will be discussed next.

The Role of Audited Financial Statements in Society

A financial statement audit is the examination of an entity's financial statements and accompanying disclosures by an independent auditor. The auditor's report must accompany the financial statements when they are issued to the intended recipients. The principal recipients are the shareholders, especially of listed companies where the audited financial statements are attached to the Annual Report of the company. In today's economy, much of the shares in listed companies are held by large shareholder investment groups such as pension funds. However, there are a significant amount of ordinary (retail) shareholders. Both these shareholder groups depend on the information provided in the financial statements for managing their portfolios.

Readers of financial statements have little option but to rely on the numbers certified as 'true and fair' by the auditors. Very little analyses can be done on the veracity of the reported numbers by the readers of the financial statements. The reason is that the audited financial statements are provided to the intended recipients in paper (word or pdf) format. In large companies these are attached to the printed Annual Reports that contain other reports such as the chairpersons statement; directors' reports; operating and financial reviews and increasingly environmental, social and governance (ESG) reports.

However, my informed view is that no Audit Committee member in any bank would have been able to spot this surge without the hindsight we now have after the fraud was discovered. The reason is that Annual Reports today have so much padding that there is little chance of discovering such anomalies.

Padding Annual Reports

Padding a report means adding unnecessary words, irrelevant data, or filler content to make a document appear longer, more substantial, or more impressive than it actually is. The primary intention or goal is often to meet a specific page count, word count, or to exaggerate the extent of work done. The key characteristics of report padding is *irrelevant information,* including extra details, unnecessary background, or extraneous charts that do not serve the purpose of the report; *redundant content* by repeating points multiple times to increase word count; and using long-winded language or excessive jargon when simple phrasing would suffice.

The ***NDB Annual Report*** *2025 is 556 pages long. There is plenty of evidence of padding*
The *Leadership* section takes 27 pages, *Operating Landscape & Strategy* (29 Pages), *Management Discussion & Analysis* (115 pages), *Risk Management & Corporate Governance* (72 pages), *Financial Statements* (148 pages), and *Supplementary Information* (129 pages).

Padding appears to be a trend in many countries in which professional bodies such as the Institutes of Chartered Accountants give awards for the *'Best Annual Report*" in various categories. Irony is that although many of the Annual Reports claim green credentials and what they did to safeguard the environment, their reports are printed and distributed thus affecting countless trees.

Simplified Reporting

The Annual Report should be regarded as an item of 'news', principally to the company's shareholders. They should be easy to read and digest just like an online newspaper article. Today, we have the technology to easily show the readers of Annual Reports what the results of *alternative policy choices* and their impact on the financial statement 'bottom lines' would be, just like journalists give interpretations and analyses of the news.

Financial Statements in Excel: Ideally, financial statements should also be presented in *Excel,* so that simple analyses could be performed. Some listed companies around the world do present their Financial Statements in the Excel format on their corporate webpages, but without any equations, only numbers. Therefore, before any analysis can be done, all the equations have to be inserted at appropriate places (e.g. the addition of all current assets into a 'Current Assets' sub-total, that itself then has to be added to the 'Total Assets' total). Further, all links to the numbers appearing in the Notes will similarly need to be inserted. This is despite the fact that the final Profit & Loss account and Balance Sheet would have most likely have been done on a package (e.g. SAP, Oracle Financials, etc.) that can be downloaded as an Excel file with the equations).

Use of Emoticons: Further, the requirement of an auditor to give a single audit opinion on a set of financial statements can be replaced the preparers of the accounts making it easy for the readers by the use of 'emoticons' to signify performance in the key business areas. For example, a number indicating 'above average' performance can be accompanied by a smiley face, etc.

In other word the Annual Report should go truly digital. This will reduce the likelihood that a Rs. 13.2 billion fraud will not be notices by the regulators or the investors. *[See Ratnatunga, Janek (2016b) on these techniques of simplified reporting by applying disruptive technologies to audited financial statements].*

Conclusion

For an executive, the anxiety surrounding cybersecurity is exacerbated by the trust economy, where a single data breach can evaporate years of brand equity in an afternoon. While Gen Z executives might find a natural focus in digital technologies, Baby ***Boomers*** often face a steeper learning curve in understanding the sophisticated tactics hackers employ. Regardless of age, the mandate is clear: cybersecurity must be a core pillar of strategic planning. This requires a paranoid mindset. Leaders must move from a posture of reactive defence to one of proactive, continuous auditing and investment in cutting-edge security infrastructure.

In the case of the NDB fraud, many bankers and auditors I have talked to have described this as *"a clear violation of controls and monitoring oversight by Finance, Internal Audit, top management, and overall, the Board risk and audit committees."*

References

CBSL (2026), "The National Development Bank PLC – Internal Fraud", Regulatory Statement, *Central Bank of Sri Lanka*, April 6, https://www.cbsl.gov.lk/en/node/20190

Chandrasekera, Duruthu Edirimuni (2026), "SEC meets with NDB board on the Rs. 13.2 billion fraud" *The Sunday Times,* April 12. https://www.sundaytimes.lk/260412/news/sec-meets-with-ndb-board-on-the-rs-13-2-billion-fraud-638929.html

Daily Mirror Journalist (2026) "First hand account of NDB fraud", *Daily Mirror,* April 10. https://www.dailymirror.lk/breaking-news/First-hand-account-of-NDB-fraud/108-337697

Ferguson, Adele (2022), "Travails of an Investigative Journalist'. *CMA Hall of Fame Awards (Australia)*, November 8. https://www.accountinghalloffame.org/hall-of-fame/ms-adele-ferguson-am-2019/

Fitch (2026), "Fitch Downgrades National Development Bank's National Rating to 'A-(lka)'; Outlook Negative", *Fitch Rating Action Commentary,* 10 April. https://www.fitchratings.com/research/banks/fitch-downgrades-national-development-bank-national-rating-to-a-lka-outlook-negative-10-04-2026

Kushan, Liyana Arachchige (2026) "The Rs. 13.2 Billion NDB Bank Fraud" *LinkedIn Post,* April 10. https://www.linkedin.com/pulse/updated-rs-132-billion-ndb-bank-fraud-kushan-liyana-arachchige-nkdic/

NDB (2025) *Annual Report 2025,* National Development Bank PLC.p.556

Ratnatunga, Janek (2016a) "The Accounting Delusion: Faith and Trust in IFRS Reports", *Journal of Applied Management Accounting Research*, 14 (1): 1-22.

Ratnatunga, Janek (2016b) "Applying Disruptive Technologies to Audited Financial Statements", *Journal of Applied Management Accounting Research*, 14 (2): 1-8.

Ratnatunga, Janek (2018a) "Auditing Opinions for Sale?", *Journal of Applied Management Accounting Research*, 16 (1): 17-19.

Ratnatunga, Janek (2018b) "The Silence of the Auditors", *Journal of Applied Management Accounting Research*, 16 (1): 21-26.

Ratnatunga, Janek (2019) "Why Audit Opinions are 'Untrue' and 'Unfair'", *Journal of Applied Management Accounting Research,* 17 (2): 23-30.

Ratnatunga, Janek (2021) "Money Laundering: Fiat Currency vs Cryptocurrency", *Journal of Applied Management Accounting Research*, Winter, 19 (1), pp. 29-46.

Singleton, Tommie W. and Singleton. Aaron J. (2010) *Fraud Auditing and Forensic Accounting* (4th ed), p 264.

Sun Tzu (2003) *The Art of War.* Translated by M. A. Griffith. Oxford University Press, Oxford.