
Table of Content

1. Executive Summary	1
2. Incident at a Glance	1
3. Timeline of Cargills Bank's Official Disclosures	2
3.1 Initial Notice – 21 March 2025.....	2
3.2 Follow-Up Notice – 25 March 2025	2
3.3 Further Update – 2 April 2025.....	3
3.4 Assessment of Bank Disclosures	3
4. Independent Findings	4
4.1 Media Reporting and Attribution to Hunters International	4
4.2 Findings by Cybersecurity Researcher Dinidu Alwis	4
4.3 Findings by Cybersecurity Expert Asela Waidyalankara.....	5
5. Risk to Customers.....	5
6. Financial Impact	5
7. Conclusion	6
Appendix	7

1. Executive Summary

In March 2025, Cargills Bank of Sri Lanka became the subject of what has been described by local media, including The Morning Telegraph, as the largest data breach in Sri Lankan banking history. The bank initially disclosed the event as “unauthorized access” to its IT infrastructure, and subsequently issued a series of follow-up notices acknowledging that an unauthorized third party had claimed to have accessed and published bank data. The incident unfolded over a period of several weeks, with the bank's public position evolving from an initial, narrowly scoped disclosure to a broader acknowledgment that its information was in fact included among the data that had been circulated.

While Cargills Bank publicly detailed the remedial and legal actions it undertook, it did not disclose the specific categories of customer data affected. This report brings together the bank's own statements alongside independent reporting in order to present a fuller, more balanced picture of the incident, its handling, and its consequences. Independent investigation, supported by media reporting and disclosures from cyber security researchers, indicates that the breach was attributed to a ransomware group known as Hunters International, with approximately 1.9 TB of data (comprising roughly 1.13 million files) offered for sale on a dark web leak site. Reported exposed data includes the National Identity Card (NIC) details of at least 4,200 customers and associated ID card photographs. The incident also had a measurable financial impact, with the bank's operational expenses increasing by 25% and its liquidity coverage ratio declining by 149.44 percentage points, as reported in the bank's 2025 annual report. Together, these developments illustrate how a cyber-security incident can carry consequences that extend well beyond the immediate technical breach, touching customer trust, regulatory standing, and financial performance alike.

2. Incident at a Glance

1.9 TB Data Exposed <i>~1.13 million files</i>	4,200+ Customers Affected <i>NIC details identified</i>	Hunters International Threat Actor <i>Ransomware group</i>
--	---	--

25% Operating Expense Increase <i>Attributed to incident response</i>	↓ 149.44 pp Liquidity Coverage Ratio <i>Per 2025 annual report</i>	Section 24 Legal Action Invoked <i>Online Safety Act No. 9 of 2024</i>
--	---	---

3. Timeline of Cargills Bank's Official Disclosures

Following detection of the incident, Cargills Bank issued a sequence of public notices. Each successive statement provided incremental detail but consistently emphasized the bank's remedial actions rather than the nature of the data compromised. Reviewing these notices in sequence is useful because it shows how the bank's account of the incident developed over time, from an initial, contained description of the event to a later acknowledgment that its own data had been part of what was leaked.

3.1 Initial Notice – 21 March 2025

Cargills Bank first disclosed the event as a cybersecurity incident involving unauthorized access to a peripheral system within its infrastructure. The bank stated that it had acted swiftly to isolate the affected components, engage top-tier cybersecurity experts to assess the scope of the threat, and confirmed that there had been no disruption to banking operations. At this early stage, the bank's communication was framed primarily as a precautionary notice, intended to reassure customers that core banking services remained available while the investigation into the scope of the intrusion was still under way.

3.2 Follow-Up Notice – 25 March 2025

In a subsequent update, the bank confirmed that an unauthorized party had claimed to have accessed and published some of the bank's data. This marked a shift in tone from the initial notice, moving from a description of unauthorized access to an acknowledgment that a claim of data publication had actually been made against the bank. Cargills Bank outlined the following actions taken in response:

- Promptly isolated the suspected components and enhanced security measures.

-
- Retained internationally recognized cybersecurity specialists to investigate the incident, provide immediate incident response, safeguard the bank against further incursions, and strengthen future cybersecurity preparedness.
 - Officially reported the incident to the relevant regulatory authorities and law enforcement agencies.
 - Actively collaborated with cybersecurity experts, regulators, and law enforcement to limit the dissemination of the data.
 - Confirmed no impact on core banking systems, with customers able to conduct daily transactions without interruption.

3.3 Further Update – 2 April 2025

A third notice, dated 2 April 2025, confirmed that the bank's ongoing investigation had established that some of the bank's information was indeed included in the leaked data. This represented the clearest admission yet from the bank that the earlier claims of a data leak were substantiated, rather than merely alleged by an outside party. The bank reiterated that it had engaged a team of leading international cybersecurity specialists for investigation, containment, and strengthening of its cybersecurity framework, and stated it was reaching out individually to identified impacted stakeholders, while continuing to maintain that core banking operations remained fully secure and functional throughout.

3.4 Assessment of Bank Disclosures

Taken together, the bank's statements consistently reference its response measures – isolation of affected systems, engagement of cybersecurity experts, regulatory notification, and legal action under Section 24 of the Online Safety Act No. 9 of 2024 to curb the circulation of the data. These measures reflect a structured incident-response process and demonstrate that the bank took the matter seriously from a procedural standpoint. However, none of the notices specify the actual categories or volume of customer data that were compromised, nor do they describe the specific customer groups affected. This gap between the bank's messaging and the information later surfaced by independent sources raises questions about the transparency of the bank's public disclosures, and highlights the distinction between

communicating that an incident is being managed and communicating what, specifically, has happened to customers' information.

4. Independent Findings

To assess the incident more successfully, publicly available reporting and credible third-party sources were reviewed. This section presents those findings in a factual and measured manner, cross-referencing media coverage with observations shared directly by cybersecurity researchers who examined the leaked material. Where the bank's own notices were largely limited to procedural detail, these independent sources offer additional insight into the scale and nature of the data actually exposed.

4.1 Media Reporting and Attribution to Hunters International

The Morning Telegraph, in its coverage, described the event as the largest cyber-attack in Sri Lankan history. According to evidence cited in this reporting and corroborated by a discussion on Reddit, the party responsible for the breach was identified as the ransomware group Hunters International. A Reddit user reported that the group listed Cargills Bank's data for sale on its dark web leak site, indicating approximately 1.9 TB of data, comprising around 1.13 million files, was ready for publication. The listing itself, as circulated online, framed the disclosure as a countdown to release, suggesting that a ransom demand may have preceded the eventual publication of the data.

4.2 Findings by Cybersecurity Researcher Dinidu Alwis

Cybersecurity researcher Dinidu Alwis, who monitored the incident, published statements on his personal account regarding the leaked data. He reported having seen a Facebook post containing the National Identity Card (NIC) details of at least 4,200 customers, front and back, uploaded following the bank's 25 March filing. According to his account, this material had been circulating publicly on social media for some time before it was widely reported, indicating that the exposure was not confined to the dark web alone but had also reached more accessible public platforms. This raises material concerns regarding the security of Cargills Bank customers' personal information, particularly given how readily identifiable, government-issued identity documents can be misused once exposed.

4.3 Findings by Cybersecurity Expert Asela Waidyalankara

Cybersecurity expert Asela Waidyalankara also commented publicly on the incident, referencing reporting by Numbers.lk, which stated that the leaked data dump included ID card photographs of bank customers and described the breach as potentially the largest in the country's history. In his commentary, Waidyalankara further observed that data breaches in Sri Lanka are frequently brought to public attention by independent researchers and public-interest activists rather than through voluntary disclosure by the affected organizations themselves, pointing to a broader gap in local breach-reporting culture that extends beyond this single incident.

5. Risk to Customers

The exposure of NIC details and ID card photographs materially increases the risk of identity-based fraud. Scammers can exploit such personal data to target individuals more effectively – for example, through impersonation, social engineering, or unauthorized account access attempts. Because NIC numbers and identity document images are frequently used as verification credentials by banks, telecommunications providers, and other institutions in Sri Lanka, their exposure creates risk that extends well beyond Cargills Bank itself, potentially enabling fraud against affected customers through entirely unrelated services. This is a serious concern given that, at the time of reporting, the bank had not directly communicated the specifics of the leaked data to affected customers, despite stating its commitment to protecting customer data and privacy. Without clear, individualized notice of what data was exposed, affected customers are left with limited ability to take timely protective measures, such as monitoring for fraudulent use of their identity documents.

6. Financial Impact

The incident also carried a measurable financial cost for Cargills Bank. To maintain operational continuity throughout the attack, the bank's operating expenses increased by 25%, reflecting costs associated with incident response and remediation. This increase illustrates that, beyond the reputational dimension, cybersecurity incidents of this nature translate into direct and quantifiable costs for the

institutions involved, spanning forensic investigation, specialist engagement, system hardening, and regulatory and legal compliance.

Furthermore, according to the bank's 2025 annual report, its liquidity coverage ratio declined by 149.44 percentage points. A decline of this magnitude may signal weakened short-term financial resilience and carries the risk of eroding customer and stakeholder trust in the bank. Taken alongside the rise in operating expenses, this decline suggests that the financial consequences of the incident were not limited to one-off remediation costs, but may also have had a broader bearing on the bank's overall financial position during the period.

7. Conclusion

The Cargills Bank incident illustrates the gap that can exist between a financial institution's public communications during a cybersecurity crisis and the fuller picture that emerges through independent investigation and media scrutiny. While the bank took visible remedial steps – isolating affected systems, engaging international cybersecurity specialists, notifying regulators, and pursuing legal action under the Online Safety Act – it did not disclose the specific nature or scale of the compromised data. Independent sources, including media outlets, Reddit reporting, and named cybersecurity researchers, indicate that at least 4,200 customers' NIC details and ID card photographs were exposed, out of a reported 1.9 TB data set attributed to the Hunters International ransomware group. Beyond the reputational and customer-trust implications, the incident had a tangible financial cost, reflected in a 25% rise in operating expenses and a 149.44 percentage point decline in the bank's liquidity coverage ratio. This case underscores the importance of transparent, timely, and specific breach disclosure to customers and stakeholders alike.

Appendix



Figure 1: Cargills Bank's initial public notice, 21 March 2025.

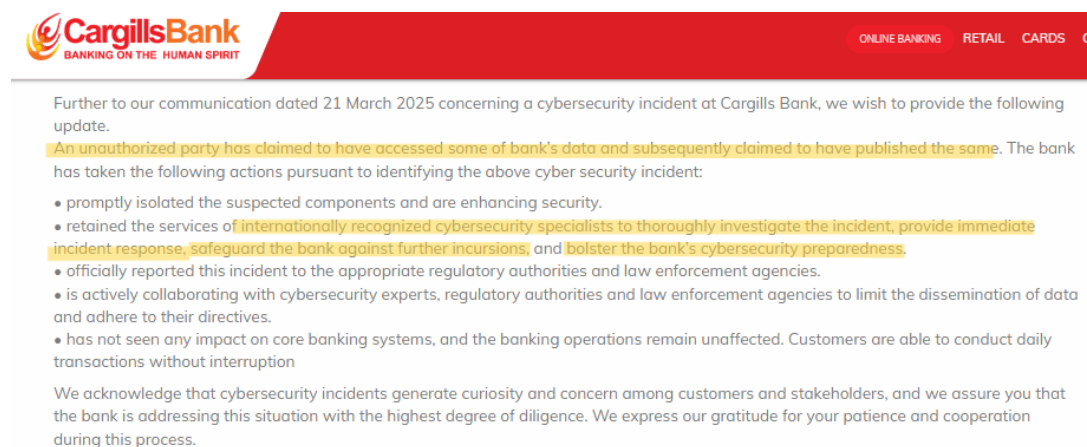


Figure 2: Cargills Bank's follow-up notice, 25 March 2025

IMPORTANT NOTICE

Dear Valued Customers,

Further to our announcements dated 21 March 2025 and 25 March 2025 regarding the cybersecurity incident at Cargills Bank PLC, we wish to provide the following update:

- As previously disclosed, an unauthorized party claimed to have accessed and published certain data belonging to the bank.
- The bank's ongoing investigation reveals that some of the bank's information is among the data.
- Upon detection of the incident, the bank engaged a team of leading international cybersecurity specialists to support our response. Their mandate includes incident investigation, containment, and strengthening of the bank's cybersecurity framework.
- The bank also immediately notified and is continuously updating regulatory and law enforcement authorities on the incident and is fully cooperating with their ongoing investigations.
- The bank is reaching out individually to identified impacted stakeholders.
- Importantly, the bank's core operations remain fully secure and functional. All banking services continue to function normally, and customers may carry out their transactions with complete confidence.

We remain fully committed to protecting our customers' data and privacy and are working closely with the relevant authorities to contain the unlawful dissemination of data and safeguard all stakeholders.



Figure 3: Cargills Bank's third public update, 2 April 2025.

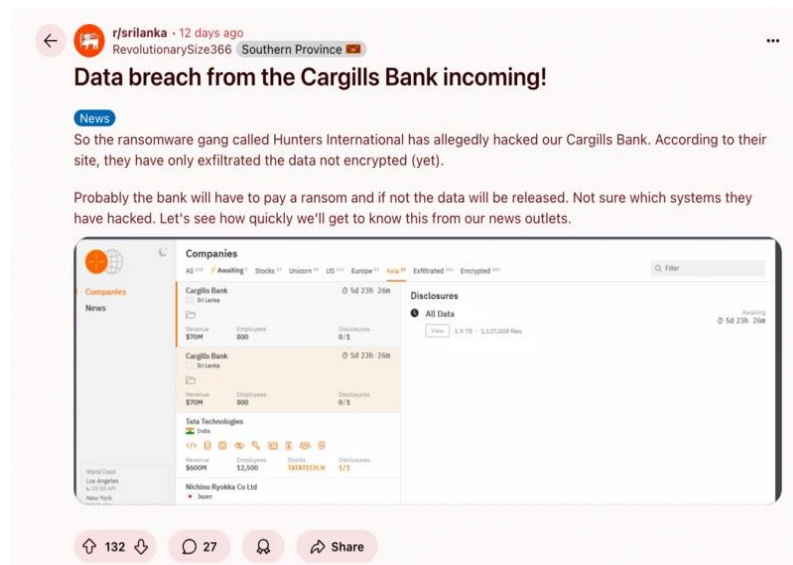


Figure 4: Reddit discussion referencing the Hunters International dark web listing for Cargills Bank.

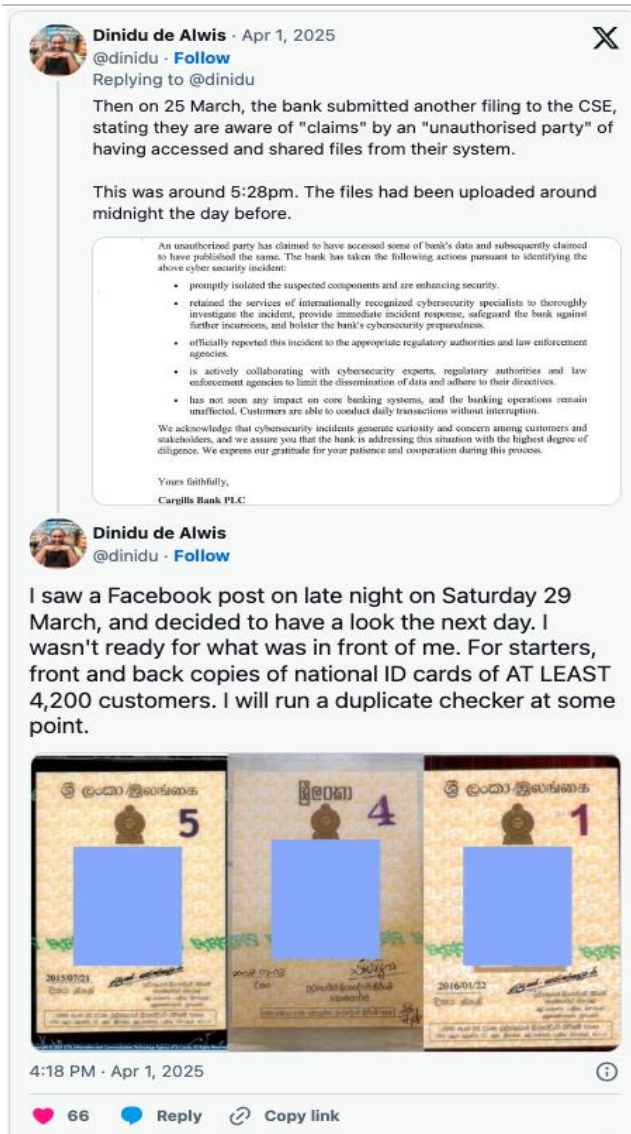


Figure 5: Social media disclosure by researcher Dinidu Alwis regarding exposed customer NIC details.

IMPORTANT NOTICE

Dear Valued Customers,

Cargills Bank has identified a cybersecurity event involving unauthorized access to a peripheral system within its infrastructure. Upon detection, we acted swiftly to fortify our systems, isolate the affected components, and engage top-tier cybersecurity experts to thoroughly assess the scope of the threat, mitigate any potential impact and safeguard the interests of our customers and the bank.

There have been no disruptions to our banking operations as a result of this event.



Figure 8: Cargills Bank's initial public notice (source screenshot).

IMPORTANT NOTICE

Dear Valued Customers,

Further to our communication dated 21 March 2025 concerning a cybersecurity incident at Cargills Bank, we wish to provide the following update.

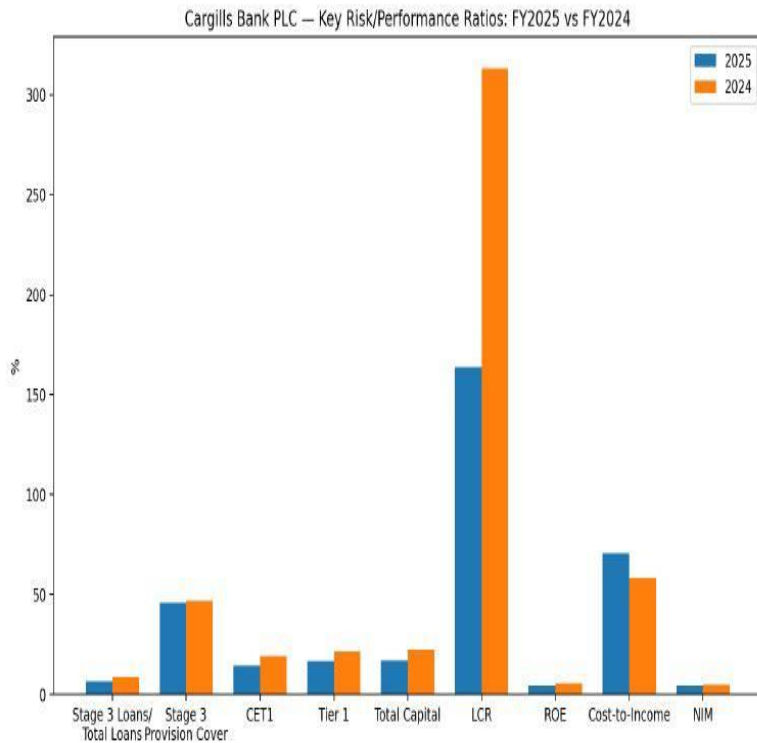
An unauthorized party has claimed to have accessed some of bank's data and subsequently claimed to have published the same. The bank has taken the following actions pursuant to identifying the above cyber security incident:

- promptly isolated the suspected components and are enhancing security.
- retained the services of internationally recognized cybersecurity specialists to thoroughly investigate the incident, provide immediate incident response, safeguard the bank against further incursions, and bolster the bank's cybersecurity preparedness.
- officially reported this incident to the appropriate regulatory authorities and law enforcement agencies.
- is actively collaborating with cybersecurity experts, regulatory authorities and law enforcement agencies to limit the dissemination of data and adhere to their directives.
- has not seen any impact on core banking systems, and the banking operations remain unaffected. Customers are able to conduct daily transactions without interruption.

We acknowledge that cybersecurity incidents generate curiosity and concern among customers and stakeholders, and we assure you that the bank is addressing this situation with the highest degree of diligence. We express our gratitude for your patience and cooperation during this process.



Figure 9: Cargills Bank's 25 March 2025 update (source screenshot).



3. Key risk, capital and performance ratios

Item	FY2025	FY2024	Unit	Change reported
Stage 3 Loans to Total Loans	6.52	8.74	%	-2.22 pp
Stage 3 Provision Cover	45.65	46.79	%	-1.14 pp
CET1 Capital Ratio	14.52	19.16	%	-4.64 pp
Tier 1 Capital Ratio	16.46	21.68	%	-5.22 pp
Total Capital Ratio	17.12	22.44	%	-5.32 pp
Liquidity Coverage Ratio	163.9	313.34	%	-149.44 pp
Return on Equity	4.51	5.42	%	-0.91 pp
Cost-to-Income Ratio	70.68	58.23	%	+12.45 pp
Net Interest Margin	4.38	4.86	%	-0.48 pp

Figure 10: 2025 annual report mention 149.44 pp decrease Of liquidity coverage ratio

reduction from 4.88% to 4.51% was witnessed reflecting the market interest environment.

Net fee and commission income of Rs. 254 Mn for the quarter ended 31 March 2025 recorded Rs. 55 Mn growth in comparison with the corresponding period in 2024. Concerted efforts to improve trade volumes, loan related fee income, card-related fee income and improved remittance income were among the main contributory factors for this growth of 28% recorded.

Capital gains realized on derecognition of financial assets boosted other income streams by Rs. 246 Mn in the quarter under review to reach Rs. 338 Mn. Net gains from financial assets at fair value through profit or loss decreased by Rs. 38 Mn to reach Rs. 46 Mn in Q1 2025. Net other operating income grew by 63% to reach Rs. 27 Mn largely due to improvement in foreign exchange gains recognized during the quarter under review.

Total operating expenses increased by 19% from Rs. 770 Mn Q1 2024 to Rs. 915 Mn in Q1 2025. Personnel expenses increased by 16% due to increase in the cadre coupled with revision in salary to reflect market conditions. Other operating expenses grew by 25% due to increase in the branch network, marketing and other administrative expenses and additional one time expenses incurred on investigations and recommendations subsequent to the Cyber Security Incident. The Bank's Cost-to-Income Ratio of 59.72% reflected a marginal increase from 58.23% in 2024.

Impairment charges totaling Rs. 126 Mn reflected a decrease of 44% from Rs. 226 Mn in the Q1 2025 subsequent to a careful scrutiny of the status of borrowers and considering the improved macro-economic environment and results of recovery actions. The Bank's Stage 3 Loans (net of Stage 3 Impairment) to Total Loans Ratio stood at 8.18% while Stage 3 Provision Cover was 46.46% as at 31 March 2025.

The Bank maintains Capital Adequacy and Liquid Assets Ratios well within the minimum requirements prescribed by the Central Bank. The Total Capital Ratio was at 19.49% while all liquidity related ratios were well above the regulatory minimum requirements.

Total assets of the Bank as at 31 March 2025 at Rs. 82.3 Bn reflected an increase of 3% or Rs. 2 Bn during the quarter. The loan book posted a moderate growth of 6%, from Rs. 46.1 Bn to Rs. 48.8 Bn, given conditions prevailing. Financial Assets measured at fair value through other comprehensive income decreased by 2% to reach Rs. 21.8 Bn. Net loss of Rs. 307 Mn was reflected in Other Comprehensive Income. Customer Deposits decreased by 5% to Rs. 56.7 Bn at the reporting date from Rs. 59.4 Bn at the end 2024.

Figure 11: 2025 annual report mention 25% operating expense increase

Group Members

1. D.M.A.D. DISSANAYAKA	2022/C/013
2. D.R.C. JAYAMAHA	2022/C/017
3. J.M.H.N. JAYALATH	2022/C/037
4. L.M.L.D. AMARASOORIYA	2022/C/048
5. M.A.B.D.C.S. APPUHAMY	2022/C/053
6. R.M.D.T. RATHNAYAKA	2022/C/072
7. T.M.H.K. SEWWANDI	2022/C/087
8. W.G.D.D.D. GUNAWARDANA	2022/C/101
9. H.G.I. SANJEEWA	2022/C/116
10. K.R.D. RAWEESHA	2022/C/117
11. N.K.M.P. NAGODA	2022/C/124
12. S.M.H. SEWMINI	2022/C/129