Telecom-Enabled Fraud in Sri Lanka: 2026 Evidence Review

Kushan Liyana Arachchige

7 September 2026

Abstract

This report examines what the public record establishes about telecom-enabled fraud in Sri Lanka and where it remains insufficient to assess institutional performance. It reviews legislation, Gazettes, parliamentary records, police releases, regulatory notices, company statements, international institutional publications and attributed reporting checked through 27 August 2026. The analysis distinguishes procedural events from findings of guilt, alleged losses from confirmed losses, and institutional positions from independent forensic evidence. It covers enforcement operations, consumer deception, payment-fraud cases, enabling infrastructure, financial redress and trafficking for forced criminality. The record documents a substantial enforcement surge: police reported 1,093 foreign-national arrests during 2026 to 13 August. Unreconciled operation counts, possible cohort overlap and incomplete case outcomes limit interpretation of that total. Published complaint figures use incompatible categories and periods and cannot establish a national fraud growth rate. Large banking-related claims require attribution and procedural qualification, while parliamentary findings identify specific public-sector control failures. Legislative and institutional changes have expanded the available response, but this review located no interoperable public series linking complaints, confirmed loss, recovery, reimbursement and case outcomes. The report recommends a common fraud data dictionary, measurable recovery and redress processes, greater transparency from communications and payment intermediaries, and individual trafficking screening in large arrest cohorts. Its findings concern the published evidence and its limitations; they do not establish national prevalence, final criminal responsibility or audited losses.

Keywords: Telecom-enabled fraud; Sri Lanka; Cybercrime; Financial fraud; Digital governance

---

Publisher: arachchi.ge; PDF edition 1.7. Originally published 4 September 2026. Evidence cut-off: 27 August 2026 (UTC).

Suggested citation: Kushan Liyana Arachchige (2026). *Telecom-Enabled Fraud in Sri Lanka: 2026 Evidence Review* (Version 1.7). arachchi.ge.

https://www.arachchi.ge/works/telecom-enabled-fraud-sri-lanka-2026/

Contents

1 Introduction

Sri Lanka has a serious telecom-enabled fraud problem. It is visible in the concentration of suspected cyber-scam operations uncovered in rented hotels, villas and apartments; in phishing sites that imitate banks and public services; and in a public-sector payment fraud that exposed basic control failures. The evidence does **not**, however, support a clean national loss total, a defensible historical claim that this is the country's "worst" telecom-fraud crisis, or a simple growth rate constructed from the complaint figures in circulation.

The most striking update is the scale of enforcement in 2026. At a police briefing on 13 August, spokesperson F. U. Wootler said **1,093 foreign nationals had been arrested during 2026** in cybercrime and financial-fraud investigations. The same briefing gave 573 arrests in 2024 and 26 in 2025. The sum of those annual reported counts is **1,692 arrests from 2024 to 13 August 2026**. Police have not published enough case-level detail to determine whether every person and cohort is unique across the underlying reports. Even the operation count differs between reports of the briefing: NewsFirst reported 27 operations[3], while Ada Derana reported 24 raids[4]. Neither account supplies a case-by-case breakdown of charges, convictions, deportations, asset recovery or trafficking screening.

That gap matters. An arrest count is not a count of convicted fraudsters, unique criminal organisations or victims protected. Some 2026 operations involved suspected computer-crime offences; others produced immigration cases. Some detainees may have been organisers or persons for whom evidence establishes knowing, uncoerced participation; the regional record also shows that people are trafficked into scam premises and forced to commit offences. The public evidence currently allows a firm conclusion about **scale and investigative pressure**, but not a firm conclusion about **criminal responsibility and outcomes** in every case.

2 Key findings

1. **The enforcement surge is real, but its meaning is unresolved.** The latest consolidated police briefing located for this review reported 1,093 foreign-national arrests in 2026 to 13 August. Public reporting does not reconcile the number of operations or show how many arrests led to computer-crime charges, immigration action, convictions, deportations or continuing investigations.
2. **"Telecom-enabled fraud" is the accurate scope.** Most conduct reviewed here is not classic fraud against a telecommunications operator. Calls, SMS, messaging apps, social platforms, online advertising, email and mobile internet are the delivery layer; payment accounts, identity records and institutional controls determine whether the attempted deception becomes a loss.

3. **The available complaint figures cannot establish a growth rate.** The often-compared totals cover different periods, institutions and categories: social-media misuse, general cybersecurity incidents, suspected financial scams and police cases. They show persistent demand on public agencies, not a consistent national time series.
4. **The largest public claims require qualification.** More than Rs6 billion allegedly lost through lookalike Commercial Bank sites remains a CID allegation reported from a preliminary court hearing. The bank says its own systems were not compromised. A threat actor's claim to have taken 1.9 terabytes from Cargills Bank was not publicly validated by the bank. By contrast, Parliament's Committee on Public Finance examined a US$2.5 million public-sector payment fraud and documented specific governance and security failures.
5. **Sri Lanka has strengthened laws and institutions, but implementation and measurement trail behind.** Caller-number manipulation intended to deceive and the use of false identity details to obtain telecom service are now specific offences. Cybercrime policing has expanded, a national security operations centre opened in 2025, and a proceeds-of-crime regime is in force. Selected core provisions of the amended Personal Data Protection Act, however, are not due to commence until 1 January 2027.
6. **Sri Lanka sits on both sides of the scam-centre economy.** Foreign nationals have been arrested in suspected centres inside Sri Lanka, while Sri Lankan nationals have been rescued from forced-criminality compounds in Myanmar. Those facts do not prove that every person arrested locally was trafficked, but they make individual screening, access to interpreters and the non-punishment principle essential safeguards.
7. **The central public-policy failure is an outcomes gap.** This review located no public, interoperable national series that joins complaints to confirmed loss, attempted loss, funds frozen, funds recovered, reimbursement, charges, convictions and deportations. Without it, raids can be counted more readily than disrupted networks or restored victims.

3 What this report means by fraud

"Telecom fraud" can describe very different harms. Interconnect bypass and SIM-box activity can deprive operators of revenue. SIM-swap abuse can defeat account controls. Phishing, impersonation and investment fraud use communications services to reach victims but normally monetise through bank accounts, cards, payment applications or cryptocurrency. A data breach may enable later fraud without itself being fraud.

This report therefore uses **telecom-enabled fraud** for deception delivered or scaled through communications and online services. It uses narrower terms where the evidence permits: phishing, business-email compromise, caller-ID manipulation, subscriber-identity

abuse, interconnect bypass, payment fraud and data breach. It does not treat every cyber incident as financial fraud, or every device seizure as proof of a particular network technique.

The distinction is not semantic housekeeping. It identifies where prevention must occur. A fake bank advertisement can involve an advertising platform, a deceptive domain, a hosting provider, an SMS or messaging channel, compromised credentials, a bank transfer, a mule account and a cash-out route. Calling the entire chain "telecom fraud" can hide the responsibilities of every participant except the carrier.

4 Method and evidence standard

This is desk research based on publicly accessible material checked through 27 August 2026. Priority was given to legislation, Gazettes, regulator and ministry notices, police releases, parliamentary records, bank statements, and publications from INTERPOL, UNODC, IOM, OHCHR and the Council of Europe. Reuters and other established news organisations were used for proceedings and events not fully documented in primary sources. Local media reports were retained where they carried a specific attributed statement or court account, but are labelled accordingly.

Claims were tested against four rules:

- an arrest, remand, charge, conviction, deportation and repatriation are different procedural events;
- a complaint, alleged loss, confirmed loss, criminal proceeds, frozen funds and recovered funds are different measures;
- an official or company statement is evidence of that institution's position, not independent proof of its forensic conclusion; and
- a regional crime pattern can inform a Sri Lankan hypothesis, but cannot establish a Sri Lankan case without local evidence.

No interviews were undertaken for this report. The right-of-reply status and response process are recorded below. No leaked personal information was accessed or reproduced. Findings that depend on unpublished case files, regulator returns or forensic reports remain open questions rather than being filled with estimates.

4.1 Review design and source selection

This is a narrative documentary review, not a systematic review or a representative survey. The unit of analysis is a published claim, measure, procedural event or institutional position relevant to communications-enabled deception and its control in Sri Lanka. Regional material is included where it helps explain a mechanism or a safeguarding issue; it is not used to establish a local case without Sri Lankan evidence. Public records and attributed

reports are retained where they identify a relevant event, legal provision, measure or stated position. General cyber incidents are distinguished from financial fraud throughout.

The reference list identifies the sources used in the report. It is not a prospective search log: a reproducible record of every search query, database result, excluded item and screening decision is not available. The review therefore makes no claim of exhaustive retrieval. Where full bibliographic details could not be established, references retain a descriptive source label and the original URL rather than supplying inferred authors or publication dates.

4.2 Comparison, reconciliation and limits

Figures are compared with their stated institution, period, category and procedural status. Conflicting accounts are reported where the available record does not reconcile them. Cohorts are not treated as unique simply because they appear in different releases, and administrative complaint counts are not converted into prevalence or loss estimates. Legislative claims distinguish enactment, commencement and implementation. Pinpoint provisions and dates are identified in the discussion where available.

The report's conclusions are an interpretation of this documentary record. There was no independent audit of institutional datasets, forensic examination of bank systems or access to complete case files. No formal review protocol, preregistration or independent duplicate screening is claimed. The right-of-reply exercise is a separate opportunity for institutions to respond to proposed findings; a response is evidence of the institution's position, and silence does not validate a claim.

5 The enforcement record: a surge measured mainly in arrests

The police's 13 August figures are the best consolidated public snapshot found in this review. Their annual reported counts - 573 foreign-national arrests in 2024, 26 in 2025 and 1,093 in 2026 to the date of the briefing - sum to 1,692, subject to the unresolved possibility of overlap in the underlying reports. The year-to-year pattern should not be mistaken for a clean crime trend. It may reflect changing enforcement intensity, changes in classification, large group arrests, immigration operations, the timing of deportations, or genuine changes in criminal presence. The public briefing does not provide the denominator needed to separate those effects.

There is also a direct inconsistency in the published record. Reuters' 30 July account described roughly 700 arrests in 2026 as "nearly double" the 2025 figure, which cannot be reconciled with the later police retrospective of 26 arrests in 2025. The difference may reflect changing definitions, an earlier denominator or a reporting error; the available sources do not resolve it.

The 2026 releases show the scale and the mixed legal basis. On 11 May, Sri Lanka Police reported 221 foreign nationals arrested across four clusters[5]: 33 people in Midigama; 55 foreign nationals and a hotel owner in Dodanduwa; 110 people in Galle; and 23 at Galle Port. Police referred to suspected offences under immigration law, the Computer Crime Act and related provisions, and reported seizures of devices and cash in some locations. These were allegations under investigation, not findings of guilt.

The need for caution was already apparent after the March operations in Anuradhapura and Mihintale. Early coverage associated 134 foreign nationals with an online-scam centre, but subsequent reporting said police had established suspected visa overstay while scam evidence had not then been confirmed[6]. In a later operation at Iranawila, Chilaw, AFP reported the arrest of 152 foreign nationals[7], with most remanded to 9 April pending investigation; another account gave 157, and no primary release located for this review reconciled the difference. The correction is not a reason to dismiss the broader pattern; it is a reason to publish charge and outcome data for each operation.

By mid-June, police had uncovered a more specific alleged fraud model in Colombo. According to The Guardian's account[8], investigators seized forged United States legal, Treasury and corporate documents and said a fictitious company had targeted US investors. The operation arrested 18 Chinese nationals and one Lao national; an unnamed investigating officer told the newspaper that police found 62 passports, mostly Chinese. The forged material and alleged target market provide more probative detail than the bare presence of phones and laptops, but the suspects were still entitled to the presumption of innocence.

In July, a murder investigation produced a tentative cybercrime lead. Reuters reported[9] that two anonymous police sources suspected the Chinese victim belonged to a larger group linked to computer scams; neither the motive nor a cybercrime connection had been established. Two people had been arrested in relation to the killing, while six others were being sought through travel restrictions and INTERPOL assistance. Reuters also reported a broader procedural pattern: many foreign nationals arrested in the cybercrime raids had appeared in court and were then deported for visa breaches or work on tourist visas. That is a meaningful enforcement result, but not the same as proving and dismantling a fraud enterprise.

INTERPOL separately reported that Sri Lanka conducted multiple raids during Operation First Light 2026 and said "hundreds" were arrested in the country[10]. The participating-country operation, funded by China's Ministry of Public Security, provides institutional corroboration rather than an independent audit. It does not resolve the Sri Lankan count, the roles of individual detainees, or the final outcomes.

5.1 Selected chronology

Table 1: Selected chronology of Sri Lanka telecom-enabled fraud enforcement and cases

Date	Publicly documented event	What the evidence establishes	What it does not establish
2024	Police later reported 573 foreign-national arrests in cybercrime and financial-fraud investigations	A substantial enforcement caseload	A common offence type, final outcomes or unique-network count
20 June 2025	Sri Lanka deported 85 Chinese nationals after proceedings connected to the 2024 Kundasale arrests [11]	Court and immigration proceedings led to removal; AFP reported visa-violation fines	Published judgments proving cybercrime convictions for all 85, or how this maps to the full 2024 cohort
3 September 2025	CID allegations concerning lookalike Commercial Bank sites were reported from Colombo Chief Magistrate's Court	A large phishing investigation entered court proceedings	A final loss, recovery, charge or conviction
19 September 2025	National Cyber Security Operations Centre opened [12]	A stated 24-hour monitoring remit over 37 critical institutions	An independently measured reduction in fraud or incidents
March-April 2026	Large foreign-national arrests in Anuradhapura/Mihintale and Chilaw	Police were later quoted as saying the March arrests rested on suspected visa overstays; devices in the later cohort were under investigation	That every detainee operated or knowingly joined a scam centre
11 May 2026	Police announced 221 arrests in four location clusters	Multiple large, coordinated investigations	Case outcomes or whether clusters formed one network
16 June 2026	Colombo raid found forged US documents; an investigating officer said police found 62 passports	A specific suspected overseas-investment deception	Conviction, victim count or loss
9 July 2026	INTERPOL described Sri Lankan raids under First Light	International operational cooperation and "hundreds" of arrests	Exact Sri Lankan arrests or asset recovery
13 August 2026	Police reported 1,093 foreign-national arrests during 2026	Latest consolidated official count located	Reconciled operation count and outcome breakdown

5.2 The missing outcome ledger

A credible enforcement account should follow a case beyond the raid. For each operation, the public should be able to see - without disclosing protected evidence - the number

of people arrested, the suspected legal basis, the number released, charged, convicted, deported or referred as potential trafficking victims, and the value of assets restrained, returned or forfeited. It should also identify whether multiple addresses belonged to one enterprise and whether local facilitators, property providers, possible pass-through account holders or controllers were investigated.

The current record is fragmented. The 2025 deportation of 85 Chinese nationals shows that some cases progressed through court and immigration proceedings. Reuters' 2026 account indicates that many others also ended in deportation for visa breaches. These outcomes may be lawful and operationally useful, but neither supports a claim that all arrestees were convicted scam operators. Nor does removal alone answer whether organisers, financial beneficiaries and infrastructure remain in place.

The description of the 85-person cohort itself illustrates the evidentiary problem. Some airport reporting called the group convicted of cybercrime and other offences. AFP's account of the same 20 June 2025 removal[11], however, said the 85 people were expelled after being fined for breaching tourist-visa conditions following the 2024 Kundasale arrests. No published judgments specifying cybercrime convictions for all 85 were located. The defensible statement is therefore that the cohort was **deported after immigration and court proceedings connected to suspected online-scam cases**, not that every member was proved to be a scam operator.

6 Relocation, cooperation and the limits of attribution

Sri Lanka's emergence as a location for suspected scam centres fits a documented international pattern: enforcement in one jurisdiction can displace mobile networks, workers and infrastructure into another. The strongest Sri Lanka-specific version of that claim comes from China, whose Ministry of Public Security has worked with Sri Lankan investigators. The nationality of detainees does not establish organisational ownership, leadership or continuity with an overseas network.

In March 2026, the Chinese Embassy in Colombo said[13] that crackdowns in Myanmar, Cambodia and elsewhere had displaced fraud groups towards other jurisdictions; it separately asserted that some gangs had moved to Sri Lanka. In a second statement in May[14], the embassy described the local increase as a spillover from regional networks and referred to several nationalities being arrested. The two governments had already placed cross-border telecom fraud and online gambling on their bilateral enforcement agenda in their January 2025 joint statement[15].

Those are relevant official assessments, but they are not independent proof that a named Southeast Asian organisation relocated intact to a named Sri Lankan address. China is also an interested law-enforcement and diplomatic actor. The proposition should remain attributed until court files, travel records, beneficial ownership, communications or financial evidence establish continuity between specific overseas and Sri Lankan networks.

The regional context is nonetheless strong. UNODC's 2026 assessment [16] describes an interconnected criminal-service ecosystem in which people from at least 80 countries and territories have been identified in Southeast Asian regional compounds and recruitment reaches well beyond the region. INTERPOL reported in 2025 [17] that trafficking victims from 66 countries had entered such centres and that operations were appearing outside their earlier geographic concentration. These sources support regional dispersion and service-based replication. The embassy remains the principal public source for a Sri Lanka-specific causal displacement claim, and neither body identifies the owners or workflow of every centre alleged locally.

Terminology should be equally careful. "Pig butchering" is often applied broadly to relationship- or investment-based online scams. INTERPOL now recommends "romance baiting" [18], both to describe the grooming mechanism more accurately and to avoid language that humiliates victims. No primary public source located for this review establishes that lifecycle for a named Sri Lankan operation. The mechanism should be used only when case evidence supports it.

7 The people at alleged scam premises: suspect, worker, trafficking victim - or more than one?

The scam-centre economy creates a dual-victim problem. People targeted by fraudulent messages lose money. Some people sending those messages have themselves been recruited through false job offers, transported, confined, assaulted and compelled to commit fraud. INTERPOL expressly cautions that not every worker is trafficked; the reverse is equally important - presence at a keyboard is not proof of free choice.

Sri Lanka has direct experience of this forced-criminality model through its own citizens abroad:

- in March 2024, the Ministry of Foreign Affairs said 56 Sri Lankans had been trafficked to four cybercrime locations in Myawaddy, Myanmar [19], with eight then rescued;
- the Ministry announced the repatriation of another 27 people in December 2024 [20];
- in February 2025 it said 91 Sri Lankans had been rescued during 2022-2024 and 18 reportedly remained [21]; and
- further releases documented 14 rescues in March 2025 [22] and 15 in May 2025 [23].

These numbers should not be added mechanically. The later rescues exceed the earlier number reported as remaining, which may reflect newly identified people, changing cohorts or inconsistent reporting. IOM provides a wider indication of exposure: by July 2026 it had assisted more than 3,500 forced-criminality trafficking victims from 39 countries during 2022-2025 [24], and Sri Lanka was among the six largest origin groups in that assisted

caseload. This is not a prevalence ranking; it is evidence that the risk is material for Sri Lankan nationals.

The local implication is procedural, not presumptive. No public raid-level screening results were found for foreign nationals detained in Sri Lanka. Investigators should therefore assess each person individually for recruitment deception, passport retention, debt bondage, restriction of movement, threats and violence; provide interpreters and legal access; and separate potential witnesses or victims from alleged organisers. Screening should occur before immigration penalties, prolonged detention or removal and should address administrative offences, safe return and non-refoulement. OHCHR's human-rights guidance[25] emphasises prompt identification and non-punishment for offences that are a direct consequence of trafficking. That principle does not preclude investigation of conduct that was not a direct consequence of trafficking. It prevents an arrest sweep from erasing the distinction.

8 What the complaint numbers do - and do not - show

Sri Lanka's public statistics are not one national fraud series. They are overlapping administrative counts produced for different purposes. The result is an apparent abundance of numbers and a shortage of comparable evidence.

Table 2: Publicly reported cyber and fraud complaint indicators

Source and period	**Published measure**	**What is included**	**Why comparison is unsafe**
CERT annual report, 2021[26]	18,214 reported incidents	16,975 social-media incidents and 1,239 other incidents	Broad administrative intake; "resolved satisfactorily" is undefined
CERT annual report, 2022[27]	16,301 reported incidents	15,674 social-media incidents and 627 other incidents	Same broad structure, but not a financial-fraud count
National Cyber Security Strategy 2025-2029[28]	4,347 incidents in 2024, including 2,241 financial scams	A much narrower strategy series, rising from 596 in 2019	Far below broad CERT intake; no published bridge or data dictionary
CERT statement, January-September 2024[29]	7,210 "online scam" complaints	Reportedly dominated by social-media matters; financial subset described inconsistently	A quoted partial-year figure with internally inconsistent category arithmetic
CERT statement, first seven months of 2025[30]	6,512 social-media cybercrime complaints, including 1,198 financial-fraud matters	Partial-year social-media intake	Not comparable with the strategy's incident series or police cases

Continued on next page

Table 2 (continued)

Source and period	Published measure	What is included	Why comparison is unsafe
CERT statement, full-year 2025[31]	More than 12,650 complaints	Social-media misuse and cybersecurity incidents, including non-fraud categories	Not a count of verified crimes, financial losses or unique victims
Public Security Minister, February 2026	23-25 cyber-related cases reported daily[32]	Ministerial estimate of daily cases reported to police	Different institution and case definition; no published reference period or deduplication method, and it should not be annualised

The 7,210 figure is particularly unstable. A CERT engineer was quoted as describing 7,210 online-scam complaints through September 2024, more than 340 financial-scam complaints and "around 20 per cent" as financial. Twenty per cent of 7,210 is about 1,442, not 340. A later article recast the partial-year number as a full-year total and used roughly 1,440 for financial fraud. Without a correction from CERT, neither reconstruction is a safe basis for a trend.

The reported figure of more than 12,650 is better supported as an aggregate, but its scope is broad: fake and compromised accounts, harassment, abusive content and misinformation can sit beside scams. Comparing it directly with 7,210 and calling the result a fraud increase would mix different periods and uncertain categories. CERT's present FAQ[33] and incident-reporting page[34] make that breadth visible: account compromise, phishing, fake profiles, cyberbullying, defamation and unauthorised access can enter its intake system. Administrative reports may also include duplicates, inquiries and events that are not ultimately verified as crimes.

Police data provides a different, equally incomplete view. In a 21 May 2026 answer to Parliament[35], the minister presented a table for the CID financial-cybercrime sub-units in seven provinces:

Table 3: Police-recorded status of financial cybercrime cases

Recorded status	2021	2022	2023	2024	2025	To 30 April 2026
Before court	0	23	10	7	7	2
Under investigation	108	166	298	683	680	144
"Resolved"	214	106	79	107	160	36

The answer did not define "resolved", say whether entries are new cases or year-end stocks, or provide investigation and prosecution durations. It also said sub-units for Uva and Sabaragamuwa were planned rather than included. The table therefore cannot

yield a clearance, prosecution or conviction rate. It does, however, expose a persistent investigation workload and the need for a standard outcomes vocabulary.

The conclusion is narrower - and more useful - than a headline growth percentage: **complaints and investigations are substantial, but this review located no published interoperable national series that can measure fraud incidence, unique victims, confirmed loss or justice outcomes over time**. This is a public-data gap; it is not proof that agencies or institutions hold no internal data.

8.1 Under-reporting cannot be converted into a loss multiplier

The claim that only 39 per cent of victims report cybercrime appears to derive from a 2023 undergraduate survey[36]. In it, 333 of 858 respondents who identified themselves as having experienced some form of cybercrime said they had reported it, or 38.8 per cent. The survey covered broad conduct such as harassment, malware and copyright violations and was not shown to be a representative national study of telecom-enabled financial fraud. Its arithmetic may be quoted as a result of that sample; it should not be presented as an official reporting rate or used to multiply complaint totals by two or three.

Exposure data also requires restraint. The Department of Census and Statistics' first-half 2025 survey[37], based on a nationally distributed sample of 12,500 households, estimated digital literacy at 70.8 per cent and internet use within the previous year at 60.4 per cent among household members aged five to 69. Digital literacy was lower among estate residents and people aged 60-69. Yet the survey defines literacy as the ability to use a digital device independently; it does not measure scam recognition, cyber hygiene, financial literacy or victimisation. These differences can guide accessible, trilingual education. They cannot establish that a demographic group is more likely to lose money.

9 Case file 1: the Commercial Bank lookalike-site investigation

The Commercial Bank case illustrates a reported phishing mechanism in which a familiar brand, a search advertisement and a payment account were combined. The bank and a CID officer said the bank's core system was not compromised; no independent forensic report was public.

On 3 September 2025, the CID was reported as telling Colombo Chief Magistrate's Court[38] that more than Rs6 billion had been siphoned through fake websites imitating ComBank Digital. Eight suspects were reported remanded later that month[39], while the court sought account information. These are significant procedural allegations. They are not a final finding that Rs6 billion was lost, that every transfer was unrecovered, or that the remanded people were guilty.

The mechanism is better established than the amount. A Fact Crescendo investigation updated in April 2026[40] documented sponsored Google results that led users to external

lookalike pages, where credentials and one-time passwords could be captured. Commercial Bank said its own systems remained secure; a senior CID officer likewise said there was no evidence of an internal bank-system hack or staff involvement at that stage. The bank said it had informed CID and CERT, pursued site takedowns and reduced its web transaction limit while recovery efforts continued.

Later reporting said a bank officer's complaint alleged that funds had been taken from 99 accounts, with losses described only as "millions"[41]. That account does not establish 99 unique customers and does not reconcile with the earlier Rs6 billion submission. No public indictment, final victim count, audited loss, recovery total, reimbursement result or conviction was located by the cut-off date.

The correct headline is therefore not "one attack stole Rs6 billion from Commercial Bank customers". It is: **CID was reported to have alleged a loss above Rs6 billion in a court investigation into lookalike banking sites; the bank says its systems were not breached, and the final loss and outcome remain unpublished**.

Commercial Bank's post-publication response of 4 September 2026 is recorded in Right of reply. It disputed unspecified social-media allegations and figures, but supplied no revised amount or supporting documentation that reconciles the figures reported above.

This distinction does not remove the bank or payment sector from the accountability chain. An external phishing site can still expose weaknesses in advertisement verification, customer warnings, transaction-risk scoring, payee checks, velocity controls, pass-through-account detection and rapid fund recall. The public record does not establish which, if any, of those controls failed in this case. The distinction locates the reported initial compromise outside the bank's core system and keeps an unresolved court allegation separate from a settled loss.

10 Case file 2: Cargills Bank - confirmed exposure, unconfirmed scale

The Cargills Bank incident belongs in this investigation because exposed identity material can create a later identity-misuse risk, not because downstream fraud has been publicly tied to the data or a telecom-fraud loss established.

On 25 March 2025, Cargills Bank said[42] an unauthorised party had claimed access to and publication of data. The bank said it isolated suspected components, engaged international specialists and informed regulators and law enforcement; its core banking system and operations were unaffected. By 8 April, the bank confirmed that some bank information was present in exposed material[43].

Hunters International reportedly claimed to possess about **1.9 terabytes and 1,137,008 files**; The Sunday Times attributed the volume to informed but unnamed sources[44]. An independent reviewer's published sample analysis[45] described identity images, onboarding videos and signature material. The bank did not publicly validate

the claimed total volume, the complete contents or the number of affected customers; the sample analysis was not independently audited. These figures establish what the attacker, unnamed sources and a reviewer claimed - not a regulator-audited universe.

The bank said it filed case 43022/1/25 and obtained a conditional order directed at websites or accounts circulating the material. Its own account of the legal action[46] cites section 24 of the Online Safety Act. The court order was not independently reviewed for this report. A blocking order can limit further circulation; it is not a judgment on the bank's security controls, notice to affected people, responsibility for harm or the attack's final scope.

No final forensic report, affected-customer total, prosecution, CBSL or data-protection enforcement outcome, or final court disposition was found. There is also no authoritative national breach register from which to establish "the largest data breach in Sri Lankan history". The defensible formulation is **a consequential publicly reported banking-data exposure**, with the attacker's claimed scale still unverified.

For fraud prevention, the unresolved questions are practical. Which identity artefacts were exposed? Were affected people told what categories concerned them? Were their accounts placed under enhanced monitoring? Were compromised identity records prevented from being reused in onboarding or SIM issuance? A takedown order does not answer these questions.

11 Case file 3: the Treasury's US$2.5 million payment loss

The strongest publicly scrutinised institutional case added since the earlier report is the Treasury's US$2.5 million debt-repayment fraud. It was not a telecom-network attack. It was a business-email-compromise-type payment-diversion case involving lookalike-domain correspondence, weak IT governance and cross-border money movement; whether an email account or system was technically compromised remained under investigation.

Parliament's Committee on Public Finance presented its report on 10 July 2026. The committee found that five instalments intended for Export Finance Australia had been redirected and identified an obsolete or unsupported Exchange environment, weak passwords, no multi-factor authentication, lookalike-domain correspondence and inadequate verification when payment instructions changed. The committee report treated the resulting US$2.5 million as a public loss[47] and described serious governance failures during the transition to the Public Debt Management Office. It left criminal responsibility and any collusion to the continuing investigation.

The CoPF report recorded official suspensions[47], and five officials were subjected to court travel restrictions[48]. Suspension and travel restrictions are protective or procedural measures, not evidence of guilt. The CID said it still needed foreign assistance and had not conclusively established every technical element of the compromise. By July, 16 terabytes of material had reportedly been sent for analysis[49]; in August, the forensic-copying process

was still reported as under way[50]. Parliament was told[51] that money had moved through accounts in several countries and that recovery was difficult.

At the cut-off, no perpetrator had been publicly convicted and no recovery had been announced. The case is nevertheless more evidentially useful than the largest public scam claims because an oversight body examined specific systems and decisions. Its lesson is basic: altered beneficiary instructions must be verified through a trusted channel independent of the email requesting the change; privileged systems need supported software and MFA; and payment approval must be governed as a security control, not treated as clerical administration.

12 Case file 4: the Postal Department's US$625,000 discrepancy

A second public-sector case shows that similar risks may persist outside central financial administration. In April 2026, Cabinet disclosed that roughly US$625,000 intended for the United States Postal Service had not reached it[52]. The Postmaster General later described[53] three suspect stages: about US$900 in 2024, more than US$400,000 in February 2025 and nearly US$190,000 in October 2025, involving email impersonation and an apparent third party. He said that, of the two larger 2025 payments, one was on hold and another was believed to have been siphoned. This was a preliminary official account, not a verified recovery or final-loss position.

On 6 May, the CID told court that no suspect had yet been identified[54] and the magistrate directed CERT to conduct on-site forensic work. United States assistance was being sought to trace and recover funds. There was no public arrest, indictment, conviction or verified recovery by 27 August. It would therefore be premature to describe the entire US$625,000 as irrecoverably stolen, but the attempted diversion and control failure warrant inclusion.

13 The mass-market playbook: impersonate, alarm, capture, move

The highest-profile institutional cases are only one layer. For individuals, the recurring pattern is simpler:

1. **Borrow authority.** Impersonate a bank, the police, the Central Bank, a delivery service or a government platform.
2. **Create urgency or fear.** Claim a traffic fine, blocked delivery, suspicious deposit, criminal investigation, expiring account or unusual transaction.

3. **Move the victim off the trusted channel.** Send a shortened link, lookalike domain, QR code, WhatsApp or Telegram contact, or arrange a video call staged to resemble an official office.
4. **Capture the control.** Obtain a password, card details, OTP, PIN, CVV, app-registration code or authorisation to install software.
5. **Monetise quickly.** Transfer to one or more accounts, buy a liquid digital asset, or direct cash elsewhere before the victim and institutions coordinate a hold.

The examples are current. In June 2026, the Ministry of Digital Economy warned of cloned GovPay pages[55] delivered through SMS and WhatsApp messages about supposed traffic fines. A 29 April Ministry notice[56] also recorded impersonation of the identity-registration department and a false e-ID application. Police described[57] schemes in which a bank impersonator handed the victim to a fake police video interrogation, complete with replica uniforms and offices, before credentials were captured and funds moved through accounts and cryptocurrency. In August, CERT said it had received complaints[58] about forged Central Bank and police letters demanding that deposit holders transfer part of their savings to a supposed investigative account.

Postal impersonation is not new, but remains active. CCID told *The Sunday Times*[59] that the postal scam was first reported in August 2023; one victim interviewed by the newspaper received a message on 9 September. By April 2024, CCID had received about 60 complaints and CERT said it had taken down five related domains. Sri Lanka Post issued another warning in March 2026[60], after further complaints and renewed circulation.

Account takeover can bypass even the visual theatre. On 14 August 2025, a CERT official was reported as describing 64 WhatsApp complaints so far that year[61], including attackers inducing people to disclose an app-verification OTP through false meeting invitations and then using the compromised account to request money from contacts. CBSL Payments and Settlements Director K. V. K. Alwis separately described lax identity checks in reported SIM-reissue cases[62], but supplied no national case or loss total. In August 2026, CERT also warned of an alleged "zero-click" WhatsApp takeover route[63], saying "many" complaints existed without publishing a count, vulnerability identifier or local forensic confirmation.

These examples do not prove that one organisation runs every scheme. They show reusable social-engineering infrastructure and the importance of response speed. Awareness is necessary, but "the customer clicked" is not an adequate systems diagnosis. Fraud succeeds when several controls fail in sequence.

14 The infrastructure claims: what the raids prove

Photographs and seizure lists from large raids are visually persuasive: rows of phones, laptops, desktops, routers and SIM cards. They establish access to communications and

computing equipment. Without forensic evidence, they do not establish how the equipment was configured, what accounts it controlled, who used it, which victims were contacted, or where criminal proceeds went.

The same rule applies to SIM boxes. A GSM gateway is not inherently fraudulent. SIM-box fraud is a gateway configuration that uses local SIMs to mask or refile traffic and bypass authorised interconnect routes. GSMA[64] and ITU-T[65] document the interconnect-bypass mechanism; INTERPOL's Operation Red Card[66] gives a separate example of a SIM-box setup used in large-scale SMS phishing. No official Sri Lankan source located for this review identified such a gateway configuration or produced routing and traffic evidence from the 2024-2026 raid equipment. Bulk devices are compatible with several legitimate and illicit configurations; forensic configuration and traffic evidence are required.

Nor does a global estimate of operator fraud establish a Sri Lankan consumer loss. Communications Fraud Control Association estimates concern revenue lost by service providers; UNODC and survey-based scam figures concern different geographies and victim concepts. None can be inserted into the national evidence as a substitute for Sri Lankan data. This report therefore does not publish a global loss number as though it measured local exposure.

15 What the legal and regulatory framework now covers

Sri Lanka is not operating without relevant law. The problem is a mix of fragmented mandates, uneven implementation and limited public outcome evidence.

15.1 Telecom offences and subscriber controls

The Sri Lanka Telecommunications (Amendment) Act No. 39 of 2024[67] was certified on **17 July 2024**, not 9 July. It is a broad sector-reform Act rather than a dedicated fraud statute, but two additions are directly relevant:

- section 46B criminalises intentional caller-number manipulation used to deceive or mislead, with a fine up to Rs10 million and/or one to three years' imprisonment; and
- section 46C criminalises wilfully providing false user-identity information to obtain telecom service, with a fine of Rs100,000 to Rs1 million and/or one to three years' imprisonment.

These provisions create clear legal hooks for caller-ID spoofing and false subscriber identity. No public prosecution or conviction series was found for either provision. Enactment alone therefore cannot show deterrence or operational use.

The wider market, licensing, commercial-5G and quality-of-service context is examined separately in Sri Lanka's telecommunications market after consolidation and commercial 5G. That market review does not assess alleged scam operations or payment losses.

Subscriber identification pre-dates the amendment. The Subscriber SIM Cards Regulations No. 1 of 2019[68] bind licensed digital-cellular operators to obtain signed retail applications, identity and address records, enter a national identity-card number before activation, upload documents, and retain corporate and end-user details for business connections. They require disconnection in specified cases, including failure to complete the required document upload within one month and departure of a registered employee from a corporate package. Registration identifies the recorded subscriber. It does not prove who is holding the device, prevent the use of stolen or proxy identities, or demonstrate that every dealer applies the rule effectively. GSMA notes that there is no empirical evidence that mandatory prepaid-SIM registration by itself reduces crime[69].

TRCSL's device-approval and IMEI service[70] allows a person to check a 15-digit IMEI by SMS to 1909 and imposes approval requirements for SIM-capable imports. TRCSL posted its individual IMEI-registration route on 29 January 2025[71]. This is a device-approval, registration and identifier-checking control that may assist investigations; the primary pages reviewed do not establish universal blocking, visitor exceptions or person-level tracing. An IMEI identifies equipment, not its human operator, and identifiers can be duplicated or tampered with; it does not stop phishing from a legitimate device or fraud conducted over Wi-Fi and online platforms. ITU's IMEI review[72] discusses the technical and attribution limits.

15.2 Payments, bank controls and consumer redress

CBSL has imposed several relevant controls, but their scope and dates need precision.

- From 1 April 2024, Payment and Settlement Systems Circular 1/2024[73] required an OTP for **every JustPay transaction equal to or exceeding Rs10,000**. The threshold includes exactly Rs10,000. Circular 1/2026[74], issued on 20 January 2026, set the JustPay maximum at Rs150,000 per transaction from 2 February; it did not expressly restate or repeal the separate OTP threshold.
- Circular 2/2024[75], mandatory from 31 March 2025, requires providers of licensed-financial-institution payment apps to obtain an accepted identity document and verify new users before allowing transactions. JustPay-enabled apps must do so before linking a current or savings account and must verify that the mobile number of the device on which the app is installed matches the number registered to that account; for existing users, the matching duty is triggered when a new account is linked. Transaction acquirers are responsible for facilitated third-party apps. Apps used solely by an e-commerce operator to collect payment for its own goods or services are excluded.
- Bank Supervision Department Circular No. 02 of 2025[76] requires licensed commercial and licensed specialised banks to notify CBSL Bank Supervision of defined IT, cyber and customer-scam incidents **within two hours of detection**. This is reporting to CBSL Bank Supervision - not a two-hour consumer-reporting rule, a public- or

customer-notification deadline, or a promise of reimbursement. The circular itself inconsistently describes the detailed-report period as 14 days in one place and 14 working days in another.

- Banking Act Direction 16/2021 [77] requires board accountability, incident response, testing and vulnerability assessment. It also requires a 24×7 security operations centre for all licensed commercial banks, domestic systemically important licensed specialised banks, and other licensed specialised banks offering electronic delivery channels beyond ATMs. A 2023 amendment [78] deferred some controls: parts of user-access and identity management and data-in-transit encryption to 31 December 2026, and independent external penetration testing on production systems to 31 December 2028. The existence of the direction must not be reported as proof that every control was fully implemented at the cut-off.

Consumer redress is stronger on paper than a simple "victim bears the loss" description suggests. Within the Regulations' defined perimeter of CBSL-regulated financial service providers, Regulation 48 of the Financial Consumer Protection Regulations No. 1 of 2023 [79] makes a provider liable for consumer loss caused by fraud, misappropriation or misuse unless it is proved that the loss occurred because of the consumer's negligence or fraudulent behaviour. This creates a default liability rule subject to a proved consumer-negligence or fraud exception; the regulation does not expressly allocate the proof burden or define its application to authorised-push-payment scams.

The same regulations require a provider to resolve a complaint within 21 calendar days. If it cannot, it must notify the complainant before the deadline, explain the reasons and steps taken, and may extend the process for no more than three months. A consumer may escalate to CBSL within a year of first complaining to the provider. CBSL's written determination is due within 90 days once complete information is available, subject to extension for complexity; it may order compensation or a refund, and binds the provider if the consumer accepts it. In May 2026, CBSL launched a complaint portal accessible 24/7 [80]. Its Financial Consumer Relations Department also publishes hotline 1935. No consolidated public dataset was found showing complaints by scam type, provider decisions, reimbursement values, reasons for denial, recovery or time to resolution.

15.3 Following the money

Sri Lanka's anti-money-laundering and customer-due-diligence framework contains controls relevant to suspected mule or pass-through accounts. The Financial Institutions (Customer Due Diligence) Rules No. 1 of 2016 [81], as amended in 2018 by Gazette 2092/02 [82], prohibit anonymous, fictitious and number-only accounts, require identification of customers and beneficial owners, and require monitoring and investigation of unusual or complex activity. No public FIU, bank or police source located for this review links the domestic raid cases to identified local mule accounts.

The framework changed materially just before this report's cut-off. The Financial Transactions Reporting (Amendment) Act No. 17 of 2026[83], certified on 4 August, puts risk-based due diligence more firmly into statute. After forming the statutory suspicion, a covered "Institution" must report a transaction or attempted transaction as soon as practicable and no later than two working days. On the statutory grounds in amended section 15 and following a suspicious-transaction report, the FIU head may direct an institution to suspend or not proceed with the suspect transaction or attempt, another transaction involving the affected funds, or the associated account for up to 14 working days. Administrative monetary-penalty ceilings for non-compliance with the Act are Rs100 million per case or instance, or Rs200 million for a subsequent contravention; these are not penalties for the underlying scam itself.

The Proceeds of Crime Act No. 5 of 2025 was certified on 30 April 2025. Gazette Extraordinary No. 2438/24 of 27 May 2025[84], made under section 1(2), appointed 1 June 2025 as the date on which the Act's provisions other than section 1 came into operation; the police opened the Proceeds of Crime Investigation Division on 20 October 2025[85]. The regime adds restraint and recovery machinery. These powers are important because a raid that removes workers but does not trace or recover the proceeds may leave the enterprise's economic centre intact. Yet neither the FTRA amendment nor the Proceeds of Crime Act guarantees that a victim's funds will be found, recalled or reimbursed, and no consolidated public recovery series was located.

15.4 Cybercrime, online safety, data protection and institutions

The Computer Crime Act No. 24 of 2007[86] supplies offences and investigative mechanisms for unauthorised access, interference, interception, unlawful devices and related conduct, including an extraterritorial nexus. The Payment Devices Frauds Act No. 30 of 2006[87] separately addresses offences involving payment cards, devices and related data and provides specialist investigation and expert-assistance machinery. Sri Lanka became a party to the Budapest Convention on Cybercrime on 1 September 2015[88], the first South Asian state to do so. Accession is a cooperation mechanism, not evidence of timely electronic-evidence exchange or successful prosecution in a particular case.

The Online Safety Act No. 9 of 2024[89] remained in force at the cut-off. Section 17's online-cheating offence carries up to seven years' imprisonment and/or a Rs700,000 fine; section 18's cheating-by-personation offence carries up to three years and/or Rs300,000. Parliament passed an Online Safety (Repeal) Bill at second reading on 23 June 2026[90] and referred it to committee, but repeal had not been enacted by 27 August. Cargills Bank's blocking application was therefore made under a law that still existed, even while its future was politically contested.

Data-protection timing has also been widely misstated. Part V commenced on 17 July 2023 under Gazette 2341/59[91], followed by Parts VI, VIII, IX and X on 1 December 2023 under Gazette 2366/08[92]. A later order appointing 18 March 2025 for wider

commencement was revoked before that date took effect. Gazette 2498/16 [93], published on 22 July 2026, sets **1 January 2027** for sections 2 and 3 and Parts I and III of the amended Personal Data Protection Act. Parts II, IV and VII remained uncommenced at the cut-off. Sri Lanka therefore did not yet have its full substantive data-protection regime in force. A DPA circular issued in August 2026 [94] directs public bodies to prepare governance, audit, training and data-protection-officer arrangements; it is readiness guidance, not evidence of full enforcement.

Institutional capacity has expanded. Sri Lanka Police already had a central Computer Crime Investigation Division and opened provincial sub-units before 2026 [95], so the February 2026 discussion of a new division should not be read as the beginning of cybercrime policing. The National Cyber Security Operations Centre opened on 19 September 2025 with a stated 24-hour monitoring remit, initially over 37 critical institutions. A June 2026 Ministry circular [96] made government information- and cybersecurity-policy implementation mandatory across public authorities. No enacted general Cyber Security Act was located by the cut-off, and no independent performance evaluation shows the effect of NCSOC or the newer administrative controls on fraud.

15.5 Control map

Table 4: Telecom-enabled fraud control map

Stage in the fraud chain	**Existing control or authority**	**Principal public gap**
Spoofed call or false subscriber identity	Telecommunications Act sections 46B-46C; SIM regulations	Prosecution and enforcement metrics; dealer-compliance audit results
Scam advertisement or lookalike site	CERT/police takedown coordination; Online Safety Act offences	Platform response times, repeat-advertiser controls and public takedown outcomes
Account or app takeover	Payment-app identity matching; OTP; bank cyber directions	National SIM-swap indicators and cross-sector event sharing
Suspicious transfer or possible pass-through account	CDD, monitoring, suspicious-transaction reports, FIU suspension power	Common rapid-recall protocol and published freeze/recovery performance
Consumer loss	Provider complaint duties and Regulation 48 liability rule	Consistent decision data, reimbursement amounts and reasons for refusal
Investigation	CCID, Computer Crime Act, Budapest Convention	Case duration, charge, conviction, deportation and trafficking-screening outcomes

Continued on next page

Table 4 (continued)

Stage in the fraud chain	Existing control or authority	Principal public gap
Proceeds	Proceeds of Crime Act and specialist police division	Public restraint, forfeiture, recovery and restitution totals
Exposed personal data	PDPA preparation; bank regulatory reporting	Full commencement, affected-person notice and enforcement outcomes

16 Why the present response is not yet measurable

The state's response is often described through actions: a raid, a deportation, a new hotline, a campaign, a circular or a law. Each may be legitimate. None, alone, establishes that fewer people are losing money or that the organisers' economic capacity has been reduced.

The missing chain is straightforward:

report → verification → payment hold → investigation → charge → adjudication → restraint/recovery → reimbursement or restitution

Sri Lanka publishes fragments at nearly every stage, but no common identifier, definition or aggregate outcome joins them. CERT can report an account takeover; police may open a case; a bank may classify a suspicious transfer; FIU may receive a transaction report; a court may impose a procedural order. Without a shared measurement architecture, the same event may be counted several times while its financial and legal outcome disappears.

This also distorts institutional incentives. Arrest totals reward visible sweeps. Complaint totals reward intake. Takedown totals reward removing domains, even if replacements appear within hours. A more defensible performance system would measure time to block, proportion of funds frozen, value returned, recurrence of infrastructure, progression of cases, and treatment of coerced workers - not simply activity.

CBSL's own June 2026 policy note[97] calls for real-time monitoring, rapid response, telco action against SIM misuse, intelligence sharing, tracing, recovery and prosecution. That is directionally sound. The investigative question is whether the policy becomes a timed operating protocol with accountable owners and published results.

17 Priority reforms

17.1 Publish one fraud data dictionary and an aggregate outcomes dashboard

CBSL, Police, CERT, TRCSL and the Ministry of Digital Economy should agree a minimum record structure and a shared incident reference. The public dashboard should

be aggregated and privacy-preserving, not a central dump of victims' personal data. At minimum, it should distinguish:

- attempted and realised loss;
- funds blocked, frozen, recovered, reimbursed and restituted;
- complaint channel, delivery channel and payment channel;
- unique reports, duplicate reports and confirmed cases;
- investigation, charge, conviction, dismissal, deportation and continuing status; and
- consumer, business and public-sector victims.

Historical series should be backfilled only where categories can be reconciled. A discontinuity should be labelled rather than hidden by a neat chart.

17.2 Make the first hours operational

Sri Lanka should create an expressly authorised, time-limited interbank hold-and-recall protocol, with defined triggers, human review, audit logs, appeal and release rules, and a clear hand-off to FIU or court process. This would require clear CBSL or statutory authority; the FIU's expanded suspension power, triggered on its statutory grounds following suspicious-transaction reporting, does not itself authorise a bank to freeze a beneficiary account solely on a consumer allegation.

Banks, finance companies and payment operators should publish the median time from a verified report to beneficiary-bank notification, amount frozen as a share of amount reported, and recovery outcome. Telcos and platforms should feed high-confidence compromise signals into the same process under controlled, purpose-limited rules.

17.3 Turn Regulation 48 into visible, consistent redress

CBSL should publish anonymised determinations and provider-level aggregate data on scam complaints: whether liability was accepted, what evidence established consumer negligence, how much was reimbursed, and how long the decision took. This would show whether the default-liability rule works consistently in practice.

Sri Lanka should also consult publicly on authorised-payment scams in which the customer technically approved a transfer after deception. Singapore's Shared Responsibility Framework[98] assigns specified duties to financial institutions and telecommunications companies and provides a loss-allocation route when those duties are breached. It is a useful comparator, not a model to import unchanged. Sri Lanka's approach must fit the default-liability rule in its existing Regulation 48, its payment infrastructure, affordability and due-process protections.

17.4 Require prevention and transparency from the delivery layer

Search, social-media, messaging, hosting, domain and app-store providers should have a verified pathway for banks and public bodies to report impersonation. Regulators should seek aggregate metrics for time to remove a reported asset, repeat appearances by the same advertiser or payment destination, and the result of advertiser verification.

Telecom operators should report the volume and disposition of caller-ID manipulation alerts, suspected bulk-messaging abuse, abnormal SIM activity and high-risk number reissues. Banks should receive a privacy-controlled indicator when a customer number has just been replaced or ported, so that sensitive credential resets and unusual payments can be stepped up. This is more targeted than assuming every registered SIM is safe.

17.5 Audit the controls that already exist

TRCSL should publish compliance findings for the 2019 SIM-registration rules, including dealer failures and sanctions, without exposing subscriber data. CBSL should disclose thematic - not institution-confidential - findings from its cyber-incident returns, including recurring control weaknesses and remediation deadlines. The 31 December 2026 user-access, identity-management and data-in-transit deadlines; the specified PDPA commencement on 1 January 2027; and the 31 December 2028 production-system external-penetration-test deadline should be treated as hard implementation programmes, not future aspirations.

Public bodies handling overseas payments should immediately apply independently verified beneficiary changes, MFA, supported email infrastructure, domain monitoring, separation of duties and incident exercises. The Treasury and Postal Department cases justify a time-bound audit across ministries, departments and state enterprises rather than waiting for another loss.

17.6 Trace controllers, facilitators and proceeds - not only premises

Scam-centre investigations should follow tenancy, company ownership, recruitment, travel, telecommunications provisioning, payment accounts, cryptocurrency off-ramps and beneficial ownership. Property owners and service providers should not be presumed complicit, but unusual whole-property rentals, mass device imports and concentrated account activity can create investigatory leads.

Police and FIU should publish aggregate proceeds-of-crime outcomes: amounts restrained, forfeited, returned abroad and restored to victims. International cooperation should be assessed by response and recovery, not only by the number of joint operations.

17.7 Screen every large arrest cohort for forced criminality

Police, Immigration, labour and anti-trafficking authorities should use a standard screening protocol, independent interpreters and confidential interviews. Potential victims should be separated from alleged controllers and referred to support; persons for whom evidence

establishes knowing, uncoerced participation should remain subject to evidence-based investigation. Published operation summaries should state how many people were screened and referred, without identifying them.

17.8 Make breach response useful to the people exposed

Where identity material is compromised, affected people need category-specific notice and practical protection, not only a statement that core operations remain available. Institutions should explain whether identity documents, contact details, credentials or biometric/onboarding media were involved; what monitoring is being provided; and how future KYC attempts using those artefacts will be challenged. DPA and CBSL should align those expectations before the specified PDPA provisions commence on 1 January 2027.

17.9 Fund forensic and prosecutorial capacity against published service standards

The provincial police expansion will matter only if it shortens evidence processing and case progression. Government should publish median forensic backlogs, international-request times and case stages, while protecting active investigations. Dedicated prosecutors and trained judges may improve continuity, but a new institutional label should not substitute for service standards, disclosure and independent review.

18 If money or an account may be at risk

This is procedural information, not legal or financial advice.

1. **Contact the bank, card issuer, wallet or payment provider immediately** using the number on its official website, app or the back of the card - not a number in the suspicious message. Ask it to secure access, stop or recall the transfer, and notify the receiving institution.
2. **Preserve evidence.** Keep the message, email headers, telephone number, URL, advertisement, screenshots, account or wallet details, transaction reference and exact times. Do not forward passwords, PINs, CVVs or OTPs to anyone.
3. **Report the incident to Police.** The current police advisory provides a CCID reporting number and in-person route[99]; the Tell IGP portal[100] also accepts online complaints. Use the current official page because police directories display different numbers for different CCID functions.
4. **Report the technical or account compromise to Sri Lanka CERT** through its incident portal[34] or hotline 101. CERT is a technical incident-response body, not a police station or chargeback service.

5. **Escalate an unresolved financial complaint to CBSL.** First complain to the regulated provider; if the response is absent or unsatisfactory, use the CBSL complaint-management system[101] or Financial Consumer Relations Department hotline 1935.
6. **If a device may be compromised, disconnect it from sensitive activity** and obtain trusted technical advice before wiping it; a reset can remove evidence needed for investigation.

Fast reporting improves the chance of a hold or recall but does not guarantee recovery. Anyone claiming that a fee, tax, OTP or cryptocurrency transfer is required to release recovered funds should be treated as a potential recovery scammer.

19 What remains unknown at the cut-off

- How the 24-versus-27 operation count in the August police briefing should be reconciled, and whether the 1,093 arrests include immigration-only cases or overlapping cohorts.
- How many people arrested from 2024 to 2026 were charged with computer or financial offences, convicted, acquitted, released, deported, repatriated or identified as potential trafficking victims.
- Which alleged Sri Lankan centres used romance-baiting, task, investment, gambling or other fraud models; whom they targeted; and what losses or proceeds can be attributed to each.
- Whether any 2024-2026 raid equipment included operational SIM-box gateways, and whether identified local SIMs or payment accounts were knowingly supplied to criminal networks.
- A nationally consistent count of unique fraud victims, attempted and realised loss, recovery, reimbursement and restitution.
- The final loss, victim and recovery position in the Commercial Bank phishing investigation.
- The full validated scope, affected-person notice, regulatory outcome and court disposition in the Cargills Bank incident.
- The criminal and recovery outcomes of the Treasury and Postal Department cases.
- How often the 2024 caller-ID and false-subscriber-identity offences have been investigated, charged or adjudicated.
- Whether platform, domain, telco and bank interventions materially reduce repeat infrastructure or merely move it.

20 Conclusion

Sri Lanka's evidence supports a serious warning, but not the earlier report's clean crisis arithmetic. Police have conducted suspected cybercrime and financial-fraud operations on a scale that demands sustained attention. The 2026 arrest surge is too large to dismiss as an isolated enforcement episode, although its offence composition remains unresolved. Bank and government impersonation is current. The CoPF findings show that even a sophisticated institutional payment can fail when identity, email and verification controls are weak. At the same time, the public record does not support labelling every foreign detainee a convicted scammer, turning broad CERT intake into a fraud trend, treating a threat actor's breach claim as a forensic result, or converting a student survey into a national loss multiplier.

The most consequential finding is institutional: Sri Lanka is better at publishing **events** than **outcomes**. Raids, warnings, circulars and new powers are visible. The progression of cases, the movement and recovery of money, the consistency of consumer redress, the enforcement of telecom controls and the screening of coerced workers are not.

The next phase should be judged by fewer but harder measures: how quickly money is stopped, how much is returned, whether organisers and facilitators are proved responsible, whether repeat infrastructure is disabled, whether regulated firms meet their duties, and whether trafficked people are identified rather than processed as disposable labour. That is the difference between a crackdown and a fraud-control system.

21 About this report

Evidence cut-off: 27 August 2026 (UTC)

Edition note: Version 1.7 is an author-published research report. It has not undergone formal peer review. The evidence cut-off remains unchanged; the dated post-publication response below records correspondence received on 4 September 2026.

> **Provenance note.** This report is a distinct, re-researched companion to *An investigative report on the rise of telecom fraud in Sri Lanka - March 2026*, first published by Yunnan Gateway on 12 March 2026, reproduced on LinkedIn on 4 May 2026 [1], and catalogued at the existing arachchi.ge route [2]. It preserves that work's publication history while testing, updating and, where necessary, correcting its claims.

21.1 Limitations

- This is desk research. No interviews, victim testimony, non-public regulator returns, authenticated leaked files or subpoenaed records were available.
- Public sources were checked through 27 August 2026 UTC. Arrest and case data may change as investigations are reclassified.

- Court claims, police allegations, parliamentary findings and institutional statements are identified by source and procedural status. Published company positions are not treated as independent forensic findings.
- The absence of a public dataset or judgment means none was located in the sources searched; it does not prove that the underlying institution holds no record.
- No leaked personal data was accessed, downloaded or reproduced.

21.2 Funding, interests and assistance

No external funding, commissioning party, privileged access, relevant affiliation, or actual or perceived conflict of interest applies to this report.

AI-assisted research and drafting were used to discover sources, compare claims, reconcile contradictions and prepare the manuscript. No model output was treated as evidence; the cited sources remain the evidentiary basis of the report.

The accompanying editorial illustration was generated with AI and is conceptual. It does not depict incident locations or reconstruct documentary evidence.

21.3 Right of reply

Deadline outcome (checked after 5:00 p.m. Sri Lanka Standard Time (UTC+5:30) on 4 September 2026): The relevant proposed findings and numbered questions were sent separately through published official email channels on 28 August 2026 to Commercial Bank of Ceylon, Cargills Bank, the Central Bank of Sri Lanka, Sri Lanka Police, the Department of Immigration and Emigration, the Embassy of China in Sri Lanka, Sri Lanka CERT, the Telecommunications Regulatory Commission of Sri Lanka, the Ministry of Digital Economy, the Ministry of Finance and Public Debt Management Office, the Department of Posts and Google.

Commercial Bank sent an automated receipt acknowledgement stating that a response could be expected within two working days; no substantive response followed by the deadline. Google sent an automated acknowledgement explaining its general press-inquiry process and help channels; it did not answer the questions or expressly refuse to respond. No reply was received from the other ten recipients by the deadline. No non-delivery notice, extension request, express refusal, substantive response or factual correction was received for any of the twelve messages by that deadline. Automated acknowledgements confirm receipt by the Commercial Bank and Google mail systems; delivery to the ten silent recipients was not independently confirmed.

The author confirmed on 4 September 2026 that incoming mail to **editorial@arachchi.ge** is automatically forwarded to the connected inbox. The initial post-deadline check found no additional response. A subsequent check located the substantive Commercial Bank response summarised below; the deadline record above remains unchanged.

Post-publication response - 4 September 2026. Commercial Bank responded after the 5:00 p.m. Sri Lanka Standard Time deadline. The bank said that judicial proceedings and law-enforcement investigations were ongoing and that it could not provide specific operational details, figures or procedural information because the matter was sub judice. It also disputed allegations and figures circulating in recent social-media publications, without identifying individual publications or supplying revised figures or supporting documentation. The bank offered to communicate official public developments. This response is recorded alongside the previously published evidence; the reported amounts remain attributed allegations rather than independently established final losses.

Published statements from Commercial Bank, Cargills Bank, Sri Lanka Police, government bodies and the Chinese Embassy are included where relevant. Those statements pre-date this report and are not responses to its findings or questions. As at publication, the absence of a response from the ten silent recipients is recorded as silence, not as a refusal or as evidence for or against the report's findings.

21.4 Corrections and continuing responses

Material corrections will identify the changed claim, the prior wording, the reason and the date. New arrest totals or case developments will not be inserted without updating the evidence cut-off and checking whether the denominator and legal status changed.

Institutions and readers may continue to submit documentary responses after publication through the site's contact channel. Verified material responses will be added by dated update; disagreement alone will not displace substantiated reporting.

Version 1.0 update - 4 September 2026 (UTC). This edition adds an abstract, fuller explanation of the documentary review method, a complete reference list and a fixed PDF edition. It replaces the earlier statement that the post-deadline response audit was complete with the dated Commercial Bank response above. The original publication date, evidence cut-off and qualified case figures are retained.

Presentation revision - 4 September 2026: Version 1.1 introduces conventional scholarly typesetting, numbered sections and tables, and revised navigation. The publication and provenance notes now appear under "About this report". The evidence, case qualifications, source registry and post-publication response remain unchanged from version 1.0.

Technical revisions - 6 September 2026: Version 1.2 updates release validation and error reporting; version 1.3 adds publication-notice support; and version 1.4 clarifies the publisher information on the PDF cover. These revisions do not change the evidence, case qualifications, source registry or response history. The report has no formal correction entries.

Technical revisions - 7 September 2026: Version 1.5 added legacy-heading support. Version 1.6 adds anchor-collision checks and corrects the edition note. Version 1.7 repairs PDF outline destinations. The evidence, references and response history are unchanged.

References

Numbers identify linked sources used in this work. A source is evidence for the attributed statement; inclusion does not imply independent verification of every claim in that source.

† Descriptive source label from the report; full bibliographic metadata not independently verified.

[1] LinkedIn. *An investigative report on the rise of telecom fraud in Sri Lanka - March 2026 (LinkedIn reproduction).*†
https://www.linkedin.com/pulse/investigative-report-rise-telecom-fraud-sri-lanka-march-arachchige-envvc

[2] arachchi.ge. *An investigative report on the rise of telecom fraud in Sri Lanka - March 2026 (author's catalogue record).*†
https://www.arachchi.ge/works/telecom-fraud-sri-lanka/

[3] NewsFirst. (2026-08-13). *Sri Lanka Arrests 1,093 Foreign Nationals Linked to Cyber Crime Networks In 2026*.
https://www.newsfirst.lk/2026/08/13/sri-lanka-arrests-1-093-foreign-nationals-linked-to-cyber-crime-networks-in-2026

[4] Ada Derana. (2026-08-13). *More than 1,000 foreign nationals arrested for cybercrime and financial fraud this year: Sri Lanka Police*.
https://adaderana.lk/news/cmsrliyfo0005356qsmfhvhvx

[5] Sri Lanka Police. *Police record of the May 2026 cybercrime operations.*†
https://www.police.lk/?p=23554

[6] The Online Citizen. (2026-04-06). *Sri Lanka intensifies cybercrime crackdown with Chinese nationals detained in Chilaw raid*.
https://theonlinecitizen.com/2026/04/06/sri-lanka-intensifies-cybercrime-crackdown-with-chinese-nationals-detained-in-chilaw-raid

[7] South China Morning Post / Agence France-Presse. (2026-04-03). *Sri Lanka arrests 152 in alleged Chinese-run cyberscam*.
https://www.scmp.com/news/asia/south-asia/article/3349001/sri-lanka-arrests-152-alleged-chinese-run-cyberscam

[8] The Guardian. *Sri Lanka sees 'alarming' rise in cybercrime as scam networks relocate from south-east Asia*.
https://www.theguardian.com/world/2026/jun/16/sri-lanka-alarming-rise-cybercrime-scam-networks-south-east-asia-cambodia-myanmar-china

[9] Reuters. *Report on suspects sought in a Chinese national's murder and a possible cybercrime connection.*†
https://www.reuters.com/world/china/sri-lanka-seeks-six-suspects-chinese-nationals-murder-linked-cybercrimes-2026-07-30/

[10] INTERPOL. (2026-07-09). *Over 5,800 arrests, USD 293 million intercepted in global fraud bust*.
https://www.interpol.int/News-and-Events/News/2026/Over-5-800-arrests-USD-293-million-intercepted-in-global-fraud-bust

[11] The Express Tribune / Agence France-Presse. *Report on the deportation of 85 Chinese nationals after visa-violation proceedings.*†
https://tribune.com.pk/story/2551938/sri-lanka-deports-dozens-of-chinese

[12] Ministry of Digital Economy, Sri Lanka. *Announcement of the opening of the National Cyber Security Operations Centre.*†
https://mode.gov.lk/blog/ncsic

[13] Embassy of the People's Republic of China in Sri Lanka. *Statement on regional telecom-fraud displacement and Sri Lanka.*†
https://lk.china-embassy.gov.cn/eng/xwdt/202603/t20260318_11877034.htm

[14] Embassy of the People's Republic of China in Sri Lanka. *Statement on cross-border telecom-fraud cooperation and Sri Lanka.*†
https://lk.china-embassy.gov.cn/eng/xwdt/202605/t20260529_11921386.htm

[15] Embassy of the People's Republic of China in Sri Lanka. *China-Sri Lanka Joint Statement, January 2025.*†
https://lk.china-embassy.gov.cn/eng/zgxw/202501/t20250116_11536727.htm

[16] United Nations Office on Drugs and Crime. *Assessment of Southeast Asia's interconnected criminal economy.*†
https://www.unodc.org/unodc/en/press/releases/2026/July/new-unodc-report-reveals-scale-of-south-east-asias-ever-more-interconnected-criminal-economy.html

[17] INTERPOL. *INTERPOL account of the globalisation of scam centres.*†
https://www.interpol.int/News-and-Events/News/2025/INTERPOL-releases-new-information-on-globalization-of-scam-centres

[18] INTERPOL. *INTERPOL guidance on the term 'romance baiting'.*†
https://www.interpol.int/News-and-Events/News/2024/INTERPOL-urges-end-to-Pig-Butchering-term-cites-harm-to-online-victims

[19] Ministry of Foreign Affairs, Sri Lanka. *Statement on Sri Lankans trafficked to cybercrime locations in Myawaddy, Myanmar.*†
https://mfa.gov.lk/en/eight-sl-trafficked-to-myanmar-rescued-government-of-sl/

[20] Ministry of Foreign Affairs, Sri Lanka. *Announcement of the repatriation of 27 Sri Lankan victims from Myanmar.*†
https://mfa.gov.lk/en/twenty-seven-sri-lankan-victims/

[21] Ministry of Foreign Affairs, Sri Lanka. *Statement on the rescue and safe return of Sri Lankans from Myanmar cybercrime centres.*†
https://www.mfa.gov.lk/en/news/minister-foreign-affairs-foreign-employment-tourism-vijitha-herath-discusses-rescue-and-safe

[22] Ministry of Foreign Affairs, Sri Lanka. *Announcement of the rescue of 14 Sri Lankans from Myawaddy cybercrime centres.*†
https://www.mfa.gov.lk/en/news/14-sri-lankans-rescued-cybercrime-centres-myawaddy-myanmar

[23] Ministry of Foreign Affairs, Sri Lanka. *Announcement of the rescue and repatriation of 15 Sri Lankans from Myawaddy cybercrime centres.*†
https://www.mfa.gov.lk/en/news/15-sri-lankans-rescued-and-repatriated-cybercrime-centres-myawaddy-myanmar

[24] International Organization for Migration. *Account of forced criminality and IOM-assisted trafficking victims.*† https://www.iom.int/news/trapped-behind-scam-iom-warns-trafficking-victims-are-being-forced-scam-networks

[25] Office of the United Nations High Commissioner for Human Rights. *Human-rights-based responses to trafficking for forced criminality in cyber-scam operations.*† https://www.ohchr.org/en/documents/thematic-reports/wicked-problem-seeking-human-rights-based-solutions-trafficking-cyber

[26] Sri Lanka CERT. *Sri Lanka CERT annual report, 2021*.† https://www.cert.gov.lk/wp-content/uploads/annual_reports/2021_english.pdf

[27] Sri Lanka CERT. *Sri Lanka CERT annual report, 2022*.† https://www.cert.gov.lk/wp-content/uploads/annual_reports/Annual_Report_2022.pdf

[28] Sri Lanka CERT. *National Cyber Security Strategy 2025-2029*.† https://cert.gov.lk/wp-content/uploads/policies/National_Cyber_Security_Strategy_of_Sri-Lanka.pdf

[29] The Morning. (2024-10-10). *Over 340 online banking scams reported in 2024*. https://www.themorning.lk/articles/gIxeneuCdmm7amc9h4La

[30] NewsFirst. (2025-09-22). *Over 6,500 Cybercrime Complaints Reported in First Seven Months of the Year*. https://www.newsfirst.lk/2025/09/22/over-6-500-cybercrime-complaints-reported-in-first-seven-months-of-the-year

[31] Xinhua. (2026-01-01). *Sri Lanka records over 12,650 cyber-related complaints in 2025*. https://english.news.cn/asiapacific/20260101/c5dfdead83764f34bd1c179c1be68f90/c.html

[32] Xinhua. *Report on the statement that 23-25 cyber-related cases are reported daily in Sri Lanka.*† https://english.news.cn/20260207/fb334a016bad4b7ca61d9bd4e174450d/c.html

[33] Sri Lanka CERT. *Sri Lanka CERT frequently asked questions.*† https://cert.gov.lk/faqs

[34] Sri Lanka CERT. *Sri Lanka CERT incident-reporting routes.*† https://cert.gov.lk/report_incident

[35] Parliament of Sri Lanka. (2026-05-21). *Parliamentary Debates (Hansard), 21 May 2026: Financial Cybercrime Details*. Question 1013/2025; question at cols. 2003-2004 and answer/table at cols. 2005-2006 (PDF pp. 11-12). https://www.parliament.lk/uploads/businessdocs/english/23621_english_2026-05-21.pdf

[36] ResearchGate (repository). *Cybercrime Analysis - Sri Lanka*. Manuscript submitted 4 May 2023; repository record dated February 2024. https://www.researchgate.net/publication/378336517_Cybercrime_Analysis_-_Sri_Lanka

[37] Department of Census and Statistics, Sri Lanka. *Computer Literacy Statistics 2025: First Six Months Bulletin*. Survey scope and sample: opening page; definitions: p. 1; Table 6: p. 3; internet use: Table 8, p. 4 (printed pagination). https://www.statistics.gov.lk/Resource/en/ComputerLiteracy/Bulletins/2025-FirstSixMonths.pdf

[38] Sri Lanka Mirror. *Over Rs.06 bn. siphoned from Commercial Bank accounts!* https://srilankamirror.com/news/over-rs-06-bn-siphoned-from-commercial-bank-accounts/

[39] Sri Lanka Mirror. *08 remanded over fake ComBank website scam.* https://srilankamirror.com/news/08-remanded-over-fake-combank-website-scam/

[40] Fact Crescendo Sri Lanka. *Beware of fake lookalike websites replicating ComBank Digital!* https://srilanka.factcrescendo.com/english/insight-into-the-investigation-of-a-fake-website-scam-targeting-commercial-bank-of-ceylon-plc/

[41] Sri Lanka Mirror. *Executive Officer's complaint leads to probe into major fraud at Commercial Bank.* https://srilankamirror.com/biz/executive-officers-complaint-leads-to-probe-into-major-fraud-at-commercial-bank/

[42] Cargills Bank. (2025-03-25). *Update 2: Cyber security incident at Cargills Bank.* https://www.cargillsbank.com/news/corporate/update-2-cyber-security-incident-at-cargills-bank/

[43] Cargills Bank. *Cargills Bank statement confirming exposed information and legal action.*† https://www.cargillsbank.com/cargills-bank-takes-legal-action-after-cyberattack/

[44] The Sunday Times, Sri Lanka. *Cargills Bank's massive data breach sparks cyber security overhaul.* https://www.sundaytimes.lk/250406/business-times/cargills-banks-massive-data-breach-sparks-cyber-security-overhaul-593901.html

[45] Chanidu Madalagama / Medium. (2025-04-04). *The Cargills Bank Data Leak: Uncovering Sri Lanka's Largest Breach and the Silence Surrounding It.* https://chanidumadalagama.medium.com/the-cargills-bank-data-leak-uncovering-sri-lankas-largest-breach-and-the-silence-surrounding-it-aefee619b0e6

[46] Cargills Bank. *Cargills Bank account of legal action to prevent circulation of illegally obtained data.*† https://www.cargillsbank.com/cargills-bank-files-legal-action-to-prevent-circulation-of-illegally-obtained-data-from-cyber-attack/

[47] Parliament of Sri Lanka. (2026-07-10). *Report of the Committee on Public Finance on The Fraud Linked to Cybercrime in the US Dollar 2.5 Million Debt Repayment to Australia.* Executive summary, printed p. 1; IT-control findings, pp. 9-10; official suspensions, p. 17. https://www.parliament.lk/uploads/businessdocs/english/23870_english_2026-07-10.pdf

[48] Ada Derana. (2026-04-28). *Travel ban imposed on five officials over USD 2.5 million cyber heist.* https://adaderana.lk/news/121858

[49] Newswire. (2026-07-08). *Court orders CID to report progress in USD 2.5M treasury fraud probe.* https://www.newswire.lk/2026/07/08/court-orders-cid-to-report-progress-in-usd-2-5m-treasury-fraud-probe/

[50] Daily News, Sri Lanka. *Report on the continuing forensic copying of data in the US$2.5 million Treasury investigation.*† https://dailynews.lk/2026/08/07/breaking-news/1032382/slt-copying-data-in-us-2-5-mn-treasury-funds-hack/

[51] EconomyNext. *Sri Lanka Parliament debates $2.5mn Treasury fraud.*
https://economynext.com/sri-lanka-parliament-debates-2-5mn-treasury-fraud-280080/

[52] Xinhua. *Report on the Cabinet statement concerning the Postal Department's US$625,000 payment discrepancy.*†
https://english.news.cn/20260428/802a47c3678e460895ad6150de2314d9/c.html

[53] The Morning. *$ 625,000 cyber fraud: Fraud occurred in 3 phases during 2024/'25: Postmaster.*
https://www.themorning.lk/articles/cezMWRUmHvbHreCm6HRp

[54] Newswire. (2026-05-06). *How US$625,000 vanished from Sri Lanka's Postal Department.*
https://www.newswire.lk/2026/05/06/how-us625000-vanished-from-sri-lankas-postal-department/

[55] Ministry of Digital Economy, Sri Lanka. *Warning about cloned GovPay pages and fraudulent traffic-fine messages.*†
https://mode.gov.lk/notices/scamalert

[56] Ministry of Digital Economy, Sri Lanka. *Public notice on impersonation of the identity-registration department.*†
https://mode.gov.lk/notices/publicnotice

[57] Sri Lanka Police. *Police warning about bank and police impersonation through video calls.*†
https://www.police.lk/?p=21425

[58] Daily Mirror, Sri Lanka. (2026-08-17). *Sri Lanka CERT warns of scam impersonating Central Bank, police officials.*
https://www.dailymirror.lk/breaking-news/Sri-Lanka-CERT-warns-of-scam-impersonating-Central-Bank-police-officials/108-348263

[59] The Sunday Times, Sri Lanka. (2024-04-21). *Thousands fall prey to massive SMS fraud using Postal Dept. as a front.*
https://www.sundaytimes.lk/240421/news/thousands-fall-prey-to-massive-sms-fraud-using-postal-dept-as-a-front-554749.html

[60] Newswire. *Sri Lanka Post warns of phishing scam using fake websites.*
https://www.newswire.lk/2026/03/28/sri-lanka-post-warns-of-phishing-scam-using-fake-websites/

[61] Daily Mirror, Sri Lanka. *WhatsApp hacking wave hits Sri Lanka: many targeted in OTP scam spree.*
https://www.dailymirror.lk/print/main_image/WhatsApp-hacking-wave-hits-Sri-Lanka-many-targeted-in-OTP-scam-spree/346-316723

[62] EconomyNext. *Sri Lanka Central Bank in push to tighten SIM re-issue over mobile banking scam.*
https://economynext.com/sri-lanka-central-bank-in-push-to-tighten-sim-re-issue-over-mobile-banking-scam-162467/

[63] NewsFirst. *Sri Lanka CERT Warns of New 'Zero-Click' Attack Targeting WhatsApp Accounts of Iphone Users.*
https://www.newsfirst.lk/2026/08/12/sri-lanka-cert-warns-of-new-zero-click-attack-targeting-whatsapp-accounts-of-iphone-users

[64] GSMA. *Use of SIM boxes to bypass interconnect communications.*† https://www.gsma.com/solutions-and-impact/technologies/security/gsma_resources/fs-1-1-use-of-sim-boxes-to-bypass-interconnect-communications/

[65] International Telecommunication Union. (2026-02). *Recommendation ITU-T E.371: Deemed impermissible traffic*. February 2026 edition of Recommendation E.371. https://www.itu.int/rec/T-REC-E.371/en

[66] INTERPOL. *INTERPOL account of Operation Red Card and African cybercrime enforcement.*† https://www.interpol.int/News-and-Events/News/2025/More-than-300-arrests-as-African-countries-clamp-down-on-cyber-threats

[67] Telecommunications Regulatory Commission of Sri Lanka. (2024-07-17). *Sri Lanka Telecommunications (Amendment) Act No. 39 of 2024*. Section 30, inserting principal Act sections 46B-46C; printed pp. 37-38. https://www.trc.gov.lk/content/files/acts/39-2024_E.pdf

[68] Telecommunications Regulatory Commission of Sri Lanka. (2019-08-02). *Subscriber SIM Cards (Subscriber Identification Modules - SIM) Regulations No. 01 of 2019*. Gazette Extraordinary No. 2134/56; Schedule I, paras. 1-8, pp. 2A-3A; Schedule II, paras. 1-8, p. 3A. https://www.trc.gov.lk/content/files/gazette/SIM_Gazette_E.pdf

[69] GSMA. *Mandatory registration of prepaid SIMs: GSMA policy position.*† https://www.gsma.com/solutions-and-impact/connectivity-for-good/public-policy/mobile-policy-handbook/consumer-protection/mandatory-registration-of-prepaid-sims/

[70] Telecommunications Regulatory Commission of Sri Lanka. *TRCSL device approval and IMEI verification.*† https://www.trc.gov.lk/pages_e.php?id=63

[71] Telecommunications Regulatory Commission of Sri Lanka. *Announcement of the individual IMEI-registration route.*† https://www.trc.gov.lk/newsdetails_e.php?nid=77

[72] International Telecommunication Union. (2020-07). *Reliability of International Mobile station Equipment Identity (IMEI): ITU-T Technical Report QTR-RLB-IMEI*. Sections 5.7 and 6; printed pp. 4-6. https://www.itu.int/dms_pub/itu-t/opb/tut/T-TUT-CCICT-2020-PDF-E.pdf

[73] Central Bank of Sri Lanka. (2024-01-17). *Payment and Settlement Systems Circular No. 01 of 2024: Facilitating safer and more secure transactions via mobile payment applications*. Paragraph 2(i)-(iii), p. 1. https://www.cbsl.gov.lk/sites/default/files/cbslweb_documents/laws/cdg/psd_circular_no_01_of_2024_e.pdf

[74] Central Bank of Sri Lanka. (2026-01-20). *Payment and Settlement Systems Circular No. 01 of 2026: Maximum per transaction limit and fees for JustPay transactions*. Paragraph 2.1, p. 1; paragraph 5, p. 2. https://www.cbsl.gov.lk/sites/default/files/cbslweb_documents/laws/cdg/psd_circular_no_01_of_2026_e.pdf

[75] Central Bank of Sri Lanka. (2024-12-03). *Payment and Settlement Systems Circular No. 2 of 2024: Strengthening Customer Identification Process to Safeguard Funds in Current Accounts/Savings Accounts linked to Mobile Payment Applications*. Paragraph 2(i)-(vi), pp. 1-2; Definitions note, p. 2.
https://www.cbsl.gov.lk/sites/default/files/cbslweb_documents/laws/cdg/psd_circular_no_02_of_2024_e.pdf

[76] Central Bank of Sri Lanka. (2025-05-07). *Bank Supervision Department Circular No. 02 of 2025: Reporting of Information Technology and Cybersecurity Incidents of Licensed Banks*. Paragraphs 2-4, pp. 1-2; Table 01, p. 2; Annex 01, p. 3; Annex 02 Guidelines, p. 6.
https://www.cbsl.gov.lk/sites/default/files/cbslweb_documents/laws/cdg/bsd_circular_no_2_of_2025_e.pdf

[77] Central Bank of Sri Lanka. *Banking Act Directions No. 16 of 2021*.†
https://www.cbsl.gov.lk/sites/default/files/cbslweb_documents/laws/cdg/Banking_Act_Directions_No_16_of_2021.pdf

[78] Central Bank of Sri Lanka. *Banking Act Directions No. 5 of 2023 (amendment to technology-risk requirements)*.†
https://www.cbsl.gov.lk/sites/default/files/cbslweb_documents/laws/cdg/Banking_Act_Directions_No_5_of_2023_e.pdf

[79] Central Bank of Sri Lanka. (2023-08-09). *Financial Consumer Protection Regulations No. 1 of 2023*. Gazette Extraordinary No. 2344/17; Regulations 46-47, pp. 16A-17A; Regulation 48(i), p. 17A.
https://www.cbsl.gov.lk/sites/default/files/cbslweb_documents/laws/cdg/fcrd_regulations_no_01_of_2023_e.pdf

[80] Central Bank of Sri Lanka. *Announcement of the complaint management system for financial consumers*.†
https://www.cbsl.gov.lk/en/news/cbsl-launches-the-complaint-management-system-for-financial-consumers

[81] Financial Intelligence Unit, Sri Lanka. *Financial Institutions (Customer Due Diligence) Rules No. 1 of 2016*.†
https://fiusrilanka.gov.lk/docs/Rules/2016/1951_13/1951_13_E.pdf

[82] Financial Intelligence Unit, Sri Lanka. *FIU rules and directions index, including the 2018 customer-due-diligence amendment*.†
https://fiusrilanka.gov.lk/rules_directions.html

[83] Financial Intelligence Unit, Sri Lanka. (2026-08-04). *Financial Transactions Reporting (Amendment) Act No. 17 of 2026*. Section 9, printed pp. 11-12 (principal section 7); section 18(2)(e), pp. 33-34 (principal section 15); section 22, p. 41 (principal section 19(3)).
https://fiusrilanka.gov.lk/docs/ACTs/FTRA_Amendment_Act_No_17_of_2026/FTRA_Amendment_Act_No_17_of_2026_E.pdf

[84] Department of Government Printing, Sri Lanka. *Gazette Extraordinary No. 2438/24: Proceeds of Crime Act commencement order*.†
https://documents.gov.lk/view/extra-gazettes/2025/5/2438-24_E.pdf
The linked historical URL returned HTTP 404 during edition preparation; the text was not freshly verified.

[85] Sri Lanka Police. *Announcement of the opening of the Proceeds of Crime Investigation Division.*† https://www.police.lk/?p=16057

[86] Central Bank of Sri Lanka. (2007-07-09). *Computer Crime Act No. 24 of 2007, reproduced in CBSL Annual Report 2007, Part IV*. Act begins at printed p. III; section 2 (territorial application) and section 3 (offences), p. III. https://www.cbsl.gov.lk/sites/default/files/cbslweb_documents/publications/annual_report/archives/en/2007_16_Part_04.pdf

[87] Government of Sri Lanka. *Sri Lanka government legal index, including the Payment Devices Frauds Act No. 30 of 2006.*† https://www.gov.lk/sri-lanka1/legal

[88] Council of Europe. *Council of Europe announcement of Sri Lanka becoming a party to the Budapest Convention.*† https://www.coe.int/en/web/cybercrime/-/budapest-convention-sri-lanka-now-is-a-par-1

[89] Parliament of Sri Lanka. (2024-02-01). *Online Safety Act No. 9 of 2024*. Sections 17-18, printed pp. 13-14; section 24, printed pp. 20-22. https://www.parliament.lk/uploads/acts/gbills/english/6311.pdf

[90] Parliament of Sri Lanka. (2026-06-23). *Business of the House for June 23, 2026*. Main Business of the House for Today, item (iv). https://www.parliament.lk/en/home/parliament-news/view/5227

[91] Data Protection Authority of Sri Lanka. *Gazette Extraordinary No. 2341/59: Personal Data Protection Act Part V commencement order.*† https://www.dpa.gov.lk/Gazet/2023-07-21/2341-59_E.pdf

[92] Data Protection Authority of Sri Lanka. *Gazette Extraordinary No. 2366/08: Personal Data Protection Act institutional-parts commencement order.*† https://www.dpa.gov.lk/Gazet/2024-01-08/2366-08_E.pdf

[93] Data Protection Authority of Sri Lanka. (2026-07-22). *The Personal Data Protection Act, No. 9 of 2022: Order under subsection (3) of Section 1 (Gazette Extraordinary No. 2498/16).* Page 1A; operative commencement paragraph; signed 13 July 2026. https://www.dpa.gov.lk/Gazet/2498-16_E.pdf

[94] Data Protection Authority of Sri Lanka. (2026-08-07). *Personal Data Protection Circular No. 01/2026: Application of PDPA in the Public Sector*. Paragraphs 2.1-2.2, p. 2; 3.1-3.5, pp. 2-3; Annexure 1, p. 6. https://www.dpa.gov.lk/media/DPA_Circular_012026_E.pdf

[95] Sri Lanka Police. *Police announcement of provincial Computer Crime Investigation sub-units.*† https://www.police.lk/?p=8218

[96] Ministry of Digital Economy, Sri Lanka. *Ministry of Digital Economy circular on government information- and cybersecurity-policy implementation.*† https://mode.gov.lk/circulars/Docs/6.pdf

[97] Central Bank of Sri Lanka. *Protecting Financial Consumers from Financial Frauds and Scams: A Strategic National Priority*. Shared responsibility, PDF pp. 4-5; Figure 2, PDF p. 5. https://www.cbsl.gov.lk/sites/default/files/cbslweb_documents/statistics/otherpub/information_series_note_20260630_Protecting_Financial_Consumers_from_Financial_Frauds_and_Scams_A_Strategic_National_Priority.pdf

[98] Monetary Authority of Singapore. *Announcement of the implementation of Singapore's Shared Responsibility Framework*.† https://www.mas.gov.sg/news/media-releases/2024/mas-and-imda-announce-implementation-of-shared-responsibility-framework-from-16-december-2024

[99] Sri Lanka Police. *Police advisory with CCID reporting routes*.† https://www.police.lk/?p=25259

[100] Sri Lanka Police. *Tell IGP online complaint portal*.† https://telligp.police.lk

[101] Central Bank of Sri Lanka. *CBSL complaint-management system*.† https://reachus.cbsl.lk/

[102] Parliament of Sri Lanka. *Parliament committee reports index*.† https://www.parliament.lk/en/business-of-parliament/committees/reports

[103] Yunnan Gateway. (2026-03-12). *An investigative report on the rise of telecom fraud in Sri Lanka - March 2026*. Original publication of the March report; cited for provenance. https://www.yunnangateway.com/html/2026/jingpintj_2023_0312/125832.html