APPENDIX B: INCIDENT SIZING METHODOLOGY

B.1 Overview and Purpose

This appendix documents the methodology used to estimate the total number of Mileage Plan account compromises from the 265 publicly documented incidents. The central estimate of 26,500 total theft victims, derived from a 1% public reporting rate, is supported by empirical priors on fraud underreporting, behavioural analysis of victim incentives, platform-level concentration patterns, and corroboration from Alaska's own financial statements.

B.2 Observed Data

B.2.1 Dataset Summary

Between 1 January and 30 November 2025, this investigation identified 265 unique Mileage Plan account compromises through systematic review of public forums, social media platforms, and news sources.

Platform Distribution:

Platform	**Incidents**	**% of Total**
Reddit	114	43%
Facebook Groups	51	19%
US Card Forum	33	12%
Twitter	17	6%
LinkedIn	14	5%
Other (FlyerTalk, blogs, news)	36	14%
Total	**265**	**100%**

Quarterly Distribution:

Quarter	Documented Incidents	% of Total
Q1 2025	48	18%
Q2 2025	19	7%
Q3 2025	140	53%
Q4 2025 (to 30 Nov)	58	22%
Total	**265**	**100%**

The Q3 2025 concentration (7.4x the Q2 2025 level) aligns with the period of accounting anomalies documented in this report.

B.2.2 Incident Characteristics

Of the 80 victims who quantified their losses, the average theft was 217,831 miles. Incidents exhibited consistent patterns:

- Redemptions on oneworld partner carriers, predominantly Qatar Airways
- Premium cabin bookings on long-haul international routes
- Last-minute bookings, typically within 72 hours of departure
- No notification received by the account holder
- Discovery often weeks after fraudulent travel occurred

B.2.3 What the Dataset Represents

The 265 documented incidents represent public disclosures on relatively niche platforms by victims who chose to post about resolved incidents. The reporting rate modelled is:

> The proportion of all hacked Mileage Plan customers who subsequently made themselves discoverable as victims on one of the scraped public platforms.

This is a much stricter filter than "reported to law enforcement" or "reported to the airline."

B.3 Empirical Priors on Fraud Underreporting

B.3.1 Official Reporting Rates

Research consistently demonstrates severe underreporting of fraud and cybercrime to official channels:

- The UK Office for National Statistics estimates that only approximately 14% of fraud incidents and 7% of computer misuse incidents are reported to Action Fraud or the police.
- When the FBI infiltrated the Hive ransomware group, they found that only approximately 20% of Hive's victims had reported to law enforcement.

For relatively serious frauds that merit police involvement, underreporting to official channels is of the order of 80-90%.

B.3.2 Consumer Complaint Behaviour

Research on consumer complaint behaviour shows that the vast majority of dissatisfied customers never complain, even to the firm:

- Service marketing research frequently cites that only approximately 4% of dissatisfied customers complain to the firm (roughly 1 in 26).
- Public voicing on social media is a further subset, suppressed when the customer feels some responsibility, when resolution has already been achieved, or when they anticipate criticism from peers.

B.3.3 Loyalty Fraud as a Hidden Problem

Industry analysis describes loyalty and rewards fraud as a large, partly invisible problem:

- Global loyalty and rewards fraud is estimated at $1-3 billion annually, with airlines a prominent segment.
- Industry reports explicitly acknowledge that losses are consistently underestimated and underreported.
- Loyalty points behave like currency, yet fraud against these programmes receives less attention than card fraud despite comparable economic harm.

B.4 Behavioural Analysis: Why Public Reporting is Low

B.4.1 The Harm is Largely Reversed

Alaska restores stolen miles after identity verification. Unlike credit card disputes that may take months to resolve, Mileage Plan victims typically receive restoration within days. The residual harm is:

- Temporary loss of mile liquidity
- Time spent on telephone calls (often 1-3 hours)
- Permanent account restrictions (PIN requirement, telephone-only booking)

This is sufficient to cause annoyance but, for many, does not feel like an injustice warranting public broadcast.

B.4.2 No Additional Remedy from Posting

Public posting on Reddit, Facebook, or a Chinese-language card forum almost never changes the outcome. Victims have their miles restored before posting, and there is no plausible prospect of compensation, upgrades, or public shaming that changes their treatment.

From a rational choice perspective, this dramatically reduces the expected benefit of posting.

B.4.3 Visible Social Penalties

Analysis of Reddit threads confirms that victims are often criticised rather than supported:

- Threads contain stock lectures about password reuse and security hygiene
- Some comments are openly contemptuous, labelling victims "stupid" or "careless"
- One comment stated: "you had a crazy simple basic password that was easy to guess or reset. I'm sick of taking the slack for people who aren't careful online."

Fraud research consistently shows that embarrassment and self-blame are among the strongest inhibitors of reporting and disclosure.

B.4.4 The "One-Time Courtesy" Framing

Alaska explicitly tells victims that restoration is a "one-time courtesy" and that they may not be helped again. This framing:

- Implies the victim is partly at fault
- Encourages gratitude rather than anger
- Creates perceived risk that making a fuss will damage standing with the airline

This pushes towards compliant silence, not public denunciation.

B.4.5 Low Salience Once Resolved

Once miles are restored and no money has permanently vanished, the episode lacks narrative drama. It is something one might mention to a partner once and then forget. In complaint research terms, this is a low-salience, resolved negative event, exactly the category with the lowest public voice rates.

B.5 Platform Selection Effects

The platforms scraped represent highly non-random slices of the Mileage Plan population:

Reddit overrepresents:

- High digital literacy
- Younger and more online demographics
- Travel hackers and points hobbyists with unusually strong interest in miles

US Card Forum is both language-filtered (Chinese) and topic-filtered (credit card rewards optimisation), with approximately 12,000 weekly visitors and 30,000 registered users.

Facebook and LinkedIn are only visible if the researcher happens to be in the relevant social graph.

In hidden population terms, the dataset samples from venues that contain a disproportionate share of the most online and grievance-prone victims, and almost none of the quiet, time-poor, or less technically engaged ones.

B.6 Reporting Rate Analysis

B.6.1 Simple Reporting Rate Models

Let r = the proportion of victims who appear in the scraped dataset. The implied total victim population N = 265 ÷ r.

Assumed Reporting Rate (r)	**Implied Victims (N)**	**Interpretation**
5%	5,300	Very high reporting; implausible
2%	13,250	High reporting
1%	**26,500**	**Central estimate**
0.5%	53,000	Conservative
0.1%	265,000	Extreme underreporting

B.6.2 Evaluation of the 5% Model

5% reporting implies approximately 5,300 victims total.

Where it strains:

- 5% public posting on niche forums is materially higher than typical complaint rates even for unresolved service failures, and much higher than reporting rates for fraud to authorities.
- It would require Alaska victims to be unusually eager to complain publicly about a resolved problem, despite shame, blame, and lack of further remedy.

- In US Card Forum alone, 33 cases appear among 12,000 weekly visitors. Under 5% reporting, only 660 victims would exist in that entire group, implying implausible concentration.
- In a LinkedIn thread with 48 comments, 12 self-declared victims implies that 25% of commenters were themselves hacked. Under 5% reporting, this density is a statistical tail event.

Verdict: 5% is an upper bound, not a realistic central estimate.

B.6.3 Evaluation of the 1% Model (Central Estimate)

1% reporting implies approximately 26,500 victims total and approximately 14,000 in Q3 2025 alone (approximately 153 incidents per day).

Behavioural alignment:

- 1% public posting corresponds to 1 in 100 victims choosing to craft an online post that provides no further personal benefit. This is consistent with known voice rates for resolved problems.
- It is comfortably below the 7-14% reporting rates observed for fraud and computer misuse to official channels, which is logical because public posting on niche forums is a narrower filter than "reports to police."
- It aligns with call centre workload anecdotes. If each fraud-trained agent handles 3-5 cases per day and there are approximately 30-50 such agents across shifts, the implied daily volume is 90-250 incidents, consistent with the 1% model.

Reddit concentration test:

The r/AlaskaAirlines subreddit has 59,000 members. With 114 documented incidents from this source, the visible incidence rate is 0.19%. If the true victimisation rate among Mileage Plan members is approximately 1%, and subreddit membership correlates with Mileage Plan membership, the subreddit population would contain approximately 590 victims. With 114 posting, the posting rate among victims is 19%. This is plausible for an enthusiast community: high enough to show engagement, low enough to account for lurkers.

Verdict: 1% is the most behaviourally and statistically coherent estimate.

B.6.4 Evaluation of the 0.5% Model

0.5% reporting implies approximately 53,000 victims total.

This is the "strong underreporting but still finite" case. Arguments in favour:

- Given the incentives against public posting, 1 in 200 victims surfacing online is not unreasonable.

- Adverse event monitoring programmes comparing social media mentions with formal complaints typically find that any single channel captures only a small fraction of total events.

Arguments against:

- At 53,000 victims, the absence of visible regulatory or media attention before late 2025 creates mild tension, though this may reflect the technical opacity of loyalty programme accounting.

Verdict: 0.5% is plausible and cannot be ruled out.

B.6.5 Evaluation of the 0.1% Model

0.1% reporting implies approximately 265,000 victims, representing approximately 2% of all 12 million Mileage Plan members already hacked.

This is inconsistent with:

- The tenor of victim comments, where victims present as somewhat unlucky rather than as members of a near-universal calamity
- The required call centre volume, which would be extreme

Verdict: 0.1% is a useful thought experiment but not a realistic scenario.

B.6.6 Why 10-20% Reporting is Untenable

An alternative theory might suggest that 265 documented cases represent 10-20% of all incidents, implying only 1,300-2,650 total victims.

This hypothesis fails multiple tests:

Contradiction with fraud baselines: A 10-20% public posting rate would be 2-4x higher than the rate at which UK victims of serious fraud report to Action Fraud (13%), and substantially higher than the 7% for computer misuse.

US Card Forum concentration: 33 victims in a community of 12,000 weekly visitors. If only 2,000 total victims existed worldwide, only 5 victims would be expected in this community (assuming proportional representation). The observed 33 is 6.6x the expected value.

LinkedIn concentration: 12 victims in 48 comments (25% victim rate) in a single thread is incompatible with a small total population.

Call centre workload: One customer service representative reported handling 3-5 such cases personally each day. If 2,000 total victims existed over the entire year, that would imply

approximately 5.5 incidents per day across all channels. One agent handling 3-5 per day would be handling virtually all incidents alone, which is implausible.

Verdict: 10-20% reporting requires implausibly high public posting behaviour and is inconsistent with both qualitative evidence and quantitative clustering patterns.

B.7 Corroboration from Financial Statements

B.7.1 The Accounting Anomaly

The social media analysis provides a bottom-up estimate. Alaska's financial statements provide an independent top-down estimate.

The Q2 2025 accounting anomaly implies approximately $120-200M in unexplained balance sheet movements. If this represents fraud remediation costs (partner airline settlements for fraudulent redemptions, offset by mile reinstatements), it can be translated into an approximate number of fraudulent bookings.

B.7.2 Translation to Incident Counts

Using the observed average theft of 217,831 miles and plausible partner reimbursement costs of $0.01-0.015 per mile:

Miles per Theft	**Cost per Mile**	**Cost per Booking**	**Bookings Implied by $120M**
218,000	$0.010	$2,180	55,000
218,000	$0.0125	$2,725	44,000
218,000	$0.015	$3,270	37,000

Across reasonable assumptions, a $120M loyalty partner cost anomaly corresponds to 35,000-55,000 fraudulent partner redemptions.

B.7.3 Convergence of Estimates

Methodology	**Implied Victim Range**
1% reporting rate (bottom-up)	26,500
0.5% reporting rate (bottom-up)	53,000
$120M accounting anomaly (top-down)	37,000-55,000

The overlap in magnitude between these independent approaches is notable. It would be an extraordinary coincidence for both methods to land in the same band (26,500-55,000) if the true total were only 1,000-2,000 incidents.

B.7.4 Partner Redemption Ratio Corroboration

The partner-to-passenger redemption ratio provides additional corroboration:

Quarter	Partner ($M)	Passenger ($M)	Ratio	Z-Score
Baseline Mean (Q1 2024-Q1 2025)	-	-	0.145	-
Q2 2025	70	348	0.201	+2.95σ
Q3 2025	75	338	0.222	+4.05σ

If Q2 and Q3 2025 ratios had remained at the baseline mean, expected partner redemptions would have been $50M and $49M respectively. The actual figures were $70M and $75M. The cumulative excess of $46M aligns closely with the central fraud loss estimate ($43M based on 26,500 thefts at $1,635 average economic value).

B.8 Summary and Central Estimate

B.8.1 Synthesis of Evidence

Multiple independent lines of evidence converge on the same conclusion:

1. **External priors on fraud reporting:** Official fraud reporting rates (7-14%) and consumer complaint rates (approximately 4%) establish that underreporting is severe for all types of incidents. Public posting on niche forums is a stricter filter than official reporting.

2. **Behavioural incentives:** The specific characteristics of Mileage Plan fraud (harm reversed, blame-shifting framing, visible social penalties, no benefit from posting) create unusually strong disincentives for public disclosure.

3. **Platform concentration patterns:** The density of victims in small, specialised communities (33 in US Card Forum, 12 in a single LinkedIn thread) is incompatible with a small total population but consistent with large-scale underreporting.

4. **Accounting anomaly:** The $120-200M balance sheet anomaly mechanically implies tens of thousands of high-value partner redemptions.

5. **Partner redemption ratios:** The Q2-Q3 2025 elevation of $46M excess partner redemptions aligns with fraud-based mechanisms.

B.8.2 Central Estimate

Parameter	**Value**	**Basis**
Documented incidents	265	Dataset count
Central reporting rate	1%	Behavioural and statistical analysis
Central victim estimate	**26,500**	**265 ÷ 0.01**
Plausible range	13,250-53,000	0.5%-2% reporting rates
Average miles stolen	217,831	Sample of 80 quantified incidents
Total miles stolen (central)	5.8 billion	26,500 × 217,831
Economic value at $0.0075/mile	$43M	Central estimate

B.8.3 What This Means

The 265 publicly documented hacks represent the visible tip of a much larger iceberg. Under the central 1% reporting assumption:

- Approximately 26,500 Mileage Plan members experienced account takeover and mileage theft in 2025
- Approximately 5.8 billion miles were stolen and subsequently reinstated
- The economic cost to Alaska (at the inferred SSP of $0.0075 per mile) was approximately $43M
- This figure aligns closely with the $46M excess partner redemption cost derived independently from financial statement analysis

The convergence of bottom-up incident extrapolation and top-down financial statement analysis provides substantial confidence that the true scale of the problem is measured in tens of thousands of incidents, not thousands.