

# BAKED ALASKA

## The 10-Sigma Anomaly: Undisclosed Cybersecurity Crisis and \$120M Unexplained Balance Sheet Movements at Alaska Air Group (\$ALK)

16 December 2025

---

**DISCLAIMER:** *The author holds a short position in Alaska Air Group (ALK) and stands to profit from a decline in the share price. This report represents analysis of publicly available information, including SEC filings, public financial data, and social media documentation. It constitutes opinion, not investment advice. Management may have information not apparent from public disclosures that differs from the interpretations presented here. Management's response would be welcomed.*

---

# EXECUTIVE SUMMARY

Forensic analysis of Alaska's Q2/Q3 2025 financial statements identifies a discrete, one-quarter break in loyalty programme contract-liability economics (the 10.40 $\sigma$  issuance-to-revenue anomaly) that coincides with (i) a \$195M spike in amounts due from affinity card partners and (ii) an apparent \$120M migration into "Other Non-Current Assets" the following quarter without disaggregated explanation.

These patterns are consistent with **either** (a) a **material change** in loyalty programme estimates/allocations or partner settlement terms, **or** (b) a **presentation / classification / collectibility** issue within contract balances and partner receivables. In either case, current public disclosures do not enable investors to reconcile the movement

Simultaneously, Alaska is experiencing a systematic cybersecurity failure leading to widespread theft of members' mileage (aka Atmos) accounts, which remains unchecked as of publication.

The two discoveries may be related. If the scale of the thefts approaches our estimates, this could represent a material expense that is not clearly identifiable in Alaska's SEC filings..

## Three Independent Data Sets, One Conclusion

### 1. The 10-Sigma Accounting Anomaly

In Q2 2025, Alaska's loyalty issuance-to-revenue ratio deviated **10.40 standard deviations** (Appendix A.3 for methodology; Workbook A:Sch3 for calculation) from its historical baseline. A magnitude far beyond peer airlines' comparable ratios. The ratio immediately reverted in Q3 2025, confirming a discrete anomalous event.

### 2. The Undisclosed Balance Sheet Reclassification

A \$195M quarter-on-quarter increase in "Amounts due from affinity card partners" (from \$111M to \$306M) coincides with the loyalty liability issuance anomaly. In Q3, the balance declines by \$129M while "Other Non-Current Assets" increases by \$120M, with no disaggregated narrative identifying the nature of the movement, whether it represents cash collection, reclassification to a long-dated receivable/contract asset, or another asset category.

**The Chain of Events:** Liabilities were issued significantly below historical allocation patterns (evidenced by the 10.40 $\sigma$  revenue anomaly); the resulting receivable spike's magnitude was reduced via a mid-year retroactive reclassification; and the uncollected balance appears to have been reclassified to non-current assets without disclosure.

**Decision Tree:** Based on the published financial statements, at least one of the following must be true:

1. Alaska experienced a **material change in loyalty accounting estimates or allocation judgments** (e.g., SSP/breakage/PO allocation), which would typically require interim-period explanation of the nature and effect; **or**
2. Alaska experienced a **material change in affinity partner settlement terms / collectibility / classification** (e.g., extended terms, dispute, contract-asset conditionality), which would typically require clear presentation and liquidity discussion; **or**
3. Alaska incurred a **material issuance of loyalty obligation without corresponding consideration** (e.g., mass reinstatements/customer credits), which would require an identifiable offset in revenue or expense; **or**
4. The reported presentation does not faithfully depict the underlying transaction flows and requires correction.

Management can resolve this in a single disclosure by providing a rollforward and classification bridge for the affected contract balances and affinity receivables.

### **3. The Cybersecurity Crisis at 24x Peer Rate**

Analysis of public forums documents **265 documented account compromises** in 2025 (App. D), Alaska's normalised incident rate is **24 times higher** than peer airlines. A statistically significant **\$45M excess** in partner airline redemptions aligns with established fraud underreporting rates (App. B) implying a total of **26,500 total victims** producing an estimated direct cost of **\$43M**. A convergence that transforms circumstantial evidence into a quantified correlation.

Estimated Financial Exposure

Category	Conservative	Central	Aggressive
Direct Fraud Losses	\$22M	\$43M	\$87M
Reclassification/Impairment	\$60M	\$134M	\$178M
Regulatory Penalties	\$18M	\$58M	\$125M
Litigation Reserves	\$15M	\$67M	\$303M
TOTAL	\$115M	\$302M	\$693M

App. F; WB A: Sch7

Materiality Context

Metric	Conservative	Central	Aggressive
As % of 2024 Net Income	29.0%	76.2%	175.5%
As % of 2024 Total Revenue	1.1%	2.9%	6.7%
As % of 2024 Total Assets	0.5%	1.3%	3.0%

---

# THE 10.40 $\sigma$ ANOMALY

## The Metric

The issuance-to-revenue ratio tracks loyalty liability created relative to revenue recognised. In a mature programme with stable contract economics, this ratio exhibits minimal variance.

## The Data

For 11 quarters (Q3 2022 – Q1 2025), the ratio was stable: **mean 1.883, standard deviation 0.083**.

**In Q2 2025, the ratio spiked to 2.743.**

Metric	Q2 2025
Loyalty points issued	\$576M
Loyalty other revenue	\$210M
Ratio	2.743
Deviation from baseline	<b>+10.40<math>\sigma</math></b>

*Source: Alaska Air Group Q2 2025 10-Q, Note 3: Revenue*

The ratio reverted to 1.87 in Q3 - confirming a discrete event. If the baseline ratio had held, expected issuance would have been \$396M. The **\$180M excess** requires explanation.

One mechanism that can increase loyalty contract liability without contemporaneous “loyalty programme other revenue” is issuance **without consideration** (e.g., reinstatements/customer credits following account compromise or operational correction). **However, if this is the explanation at the observed scale, it necessarily implies a corresponding offset in an identifiable income statement line (contra-revenue or expense) and would be expected to be explainable through interim disclosures.** (See Appendix A.8.)

## Peer Comparison

Airline	Q2 2025 Ratio	Baseline Mean	Z-Score
<b>Alaska</b>	<b>2.743</b>	<b>1.883</b>	<b>+10.40<math>\sigma</math></b>
United	1.20	1.199	0.01 $\sigma$
Delta	1.44	1.359	+1.33 $\sigma$
American	1.18	1.358	-0.47 $\sigma$

*\*Source: Company 10-Q filings. App. A.4 for peer comparison methodology*

The anomaly is unique to Alaska. No industry-wide factor explains the deviation.

---

# THE BALANCE SHEET TRAIL

## Step 1: The Receivable Spike (Q2 2025)

The Q2 increase in “Amounts due from affinity card partners” (+\$195M) is similar in magnitude to the ~\$180M “excess” loyalty contract liability creation implied by the issuance-to-revenue anomaly. This pairing suggests the anomaly likely flowed through the affinity channel rather than being a standalone loyalty accounting artifact.

Under ASC 606, affinity arrangements typically create (i) a receivable/cash flow from the partner and (ii) recognised “loyalty programme other revenue” alongside (iii) a contract liability for the portion of consideration allocated to future travel. The observed quarter shows an outsized liability creation relative to recognised loyalty other revenue, which is difficult to reconcile without a material change in allocation estimates/terms or an issuance event not supported by contemporaneous consideration.

## Step 2: The Reclassification (Q3 2025)

The receivable dropped by \$129M in Q3. If this represented straightforward cash collection, the cash flow statement would be expected to evidence a corresponding operating cash inflow associated with receivable movements. Appendix A notes that Q2 reflected a ~\$171M operating cash use tied to receivable movements, whereas Q3 does not evidence a comparably clear reversal.

Instead, “Other Non-Current Assets” rose by \$120M, with no disclosure describing the nature of that increase.

## Step 3: The Retroactive Revision

Alaska revised its 31 December 2024 affinity receivables from \$118M to \$176M - a **49% (\$58M) increase** - characterised as “[immaterial](#).”

The magnitude and nature of the \$58 million adjustment would ordinarily prompt a SAB 99 style materiality assessment. Such an assessment considers not only quantitative magnitude, but also qualitative factors including the nature of the item, its timing, the circumstances giving rise to the adjustment, and whether it masks trends or affects compliance with covenants or other metrics. The issue is therefore not whether a percentage threshold is crossed, but whether the adjustment is material in context.

Even if total receivables were unchanged, **a retroactive reclassification that materially alters the apparent growth rate of the same line item that spiked in the anomaly quarter is qualitatively material to trend analysis and warrants clear explanation.**

**The reclassification occurred in the Q2 10-Q filing (August 2025) - after the Q2 receivables spike to \$306M, not during the annual audit (February-March 2025).** The timing

raises questions about whether the reclassification had the effect of reducing the apparent magnitude of the Q2 spike: without revision, the increase would have been 159% (\$118M → \$306M); with revision, it was 74% (\$176M → \$306M).

## The Affinity Partner Settlement Question

The balance sheet pattern creates a narrow set of explanations that are **observable and falsifiable** under GAAP:

- **Cash collection:** If the Q3 decline reflects collection, management can reconcile cash receipts from affinity partners to operating cash flow and working capital movements.
- **Extended terms / long-dated receivable:** If payment terms extended beyond one year, the balance should remain clearly identifiable as a receivable (current vs noncurrent) with discussion of liquidity effects and any significant financing component.
- **Contract asset conditionality:** If collection became conditional on future performance/events, the balance should be described as a contract asset with disclosure of the nature of the conditionality.
- **Collectibility / dispute:** If collectibility became uncertain, management should explain the change in risk and the accounting consequences.

The current filings do not describe which of these explains the \$120M migration into “Other Non-Current Assets.”

---

# THE CYBERSECURITY CRISIS

## 24x Peer Incident Rate

Systematic review of public forums verifiably identified **265 account compromises** in 2025 up to November 30th 2025 (WB B).

**Alaska's rate is 24 times higher than the aggregate weighted average of peer airlines.** The below table was compiled using a controlled independent methodology principally on Reddit to scholastically compare the frequency of mileage thefts.

Airline	Reports	Sub-Reddit Size	Reports per 10k Members	2FA Available
Alaska	80	60k	13.3	No
Southwest	18	89k	2.02	No
American	12	113k	1.06	Yes
Delta	11	351k	0.31	Yes
United	0	176k	0.00	Yes

*\*Source: Reddit. See App. C for methodology.*

## The Q3 Surge

Quarter	Incidents	Change
Q2 2025	19	Baseline
Q3 2025	140	<b>+637%</b>

Elevated incidents of hacked accounts continue with 39 recorded in November 2025.

## Attack Characteristics

- **Target:** Partner airlines (Qatar Airways dominates victim accounts)
- **Cabin:** Premium (Business/First)
- **Timing:** <72 hours before departure
- **Average theft:** 217,831 miles
- **Notification muzzling:** Many victims report the usual email notification, and receipt, was absent

Thefts involve cash expenses for Alaska for the reimbursement they must provide partner airlines.

## Repeated Evidence Refuting User Negligence or Credential Stuffing

**PIN Bypass:** Accounts compromised despite Alaska's mandatory PIN lock already in [place](#).

**Same-Day Repeat Compromise:** One account hacked [twice](#) in one day, with password change between incidents.

**Session Hijacking:** HackerNews user reported logging in and was randomly [granted access to other customers' accounts](#). Four months later, the vulnerability persisted.

## Implied PII Data Breach

If thousands of high balance accounts have been breached, this implies that a multiple of the accounts that have been drained must have been accessed to ascertain the points balance within. We can only speculate how many **hundreds of thousands of accounts** have been accessed. These accounts may hold:

- Passport numbers
- Date of Birth
- Address
- TSA traveller redress numbers
- Family including **Children's PII**

## Suggestion the Scale of Thefts Could Be Demand-Driven

A recent blog post by [NordVPN](#) ([archive](#)) showed Alaska miles for sale on the dark web at the astonishingly low pricing:

The screenshot shows a list of five Alaska Airlines miles accounts for sale on a dark web marketplace. Each listing includes the Alaska Airlines logo, the account type and range, the quantity available, a shopping cart icon, an envelope icon, a star icon, and the price. The first listing is expanded to show terms and contact information.

Account Type	Quantity	Price
Alaska Airlines Miles Account( 100k-200k ) Comes With: Email/User Password Loyalty Number Member Balance/Miles TERMS: X[Replacement Only when point is less than 50% of the initial balance]X X[Changing log info and reporting it, does not merit a replacement]X Contact Us If you have any issues. Thank You for Shopping With Us.	x5	\$35.00
Alaska Airlines Miles Account ( 300k-400k ) Comes With: Email/User Password Loyalty Number Member B...	x2	\$90.00
Alaska Airlines Miles Account( 200k-300k ) Comes With: Email/User Password Loyalty Number Member B...	x2	\$60.00
Alaska Airlines Miles Account ( 500k-1m ) Comes With: Email/User Password Loyalty Number Member B...	x1	\$150.00
Alaska Airlines Miles Account( 1m - 5m ) Comes With: Email/User Password Loyalty Number Member B...	x1	\$700.00

One way long haul business class flights can be bought for as little as \$35.

This level of pricing begs the question that the number of travellers willing to travel under their real name on stolen points could be the inhibition on the number of accounts compromised and drained.

If this theory holds, there is no upper bound on the number of accounts accessed or waiting to be stolen from.

## Implied Impunity

The 265 identified cases manifestly indicate 1000s that were not.

58 of the accounts reference the victim contacting Alaska prior to the flight's boarding. Separately, of the flights where the origin was identified (38 cases), 39% were in the USA. For the destination (42 cases) it was 38%.

These statistics imply detainments in the 100s. So where is news of them? Surely if Alaska goes as far to say to a Titanium (highest tier) [member](#):

*"If we find out this was you, we will peruse [sic] prosecution"*

Then they would have no trepidation in apprehending the actual thieves and prosecutions would be in the public domain. One would expect Alaska to amplify them to obliterate demand for the illicit tickets and thus the motivations for the hackers.

Were they reported? Did the tickets even get cancelled? Were TSA or CBP advised of any incoming foreign nationals arriving using fraudulent tickets?

---

# THE UNIFIED THEORY: MATCHING THE DOLLARS

## The Financial Statement Anomaly

Q2 and Q3 saw notable altered behaviour in partner redemptions.

Our statistical analysis in the Appendix enumerates what is visually apparent and takes account of any post-merger dynamic shifts to identify a \$45M delta from expected partner redemptions in relation to those on Alaska's fleet.

Quarter	Partner Redemptions	Expected (Baseline)	Excess
Q2 2025	\$70M	\$51M	\$19M
Q3 2025	\$75M	\$49M	\$26M
Total			\$45M

## Bottom-Up: The Fraud Estimate

The accounts of stolen points are temporally backwards-looking by default. As we show, statistical predictions of the total number of accounts is subject to a much wider range of potential outcomes, but a convergence of these analyses is notable.

Component	Value
Documented incidents	265
Implied total victims (1% reporting)	26,500
Average theft	217,831 miles
Value at \$0.0075/mile	\$43M

## The Convergence

Methodology	Estimate
Bottom-up (incident extrapolation)	\$43M
Top-down (excess partner redemptions)	\$45M
Alignment	95%

This convergence is suggestive but should be interpreted with caution given the wide confidence interval on the bottom-up estimate.

However, two independent approaches - social media documentation and SEC filings - converge on similar figures. In my opinion, this alignment is unlikely to be coincidental.

---

# THE ALASKA RESPONSE

The documented incidents have generated observable corporate responses. The nature and timing of these responses raise questions.

Victim documentation reveals standardised response:

1. Miles restored upon identity verification
2. Characterised as "one-time courtesy"
3. Warning: "We will not help you again"
4. Victim's accounts are sanctioned with telephone-only access to book award miles.

The consistency suggests formal policy designed to meet frequent incidents. One CSR is quoted saying on hacked account victims "[\*she has to do this 3-5 times per day\*](#)".

## The Terms Change in Apparent Response

Alaska very recently changed the terms to their loyalty program with just one non-immaterial alteration, the addition of [a standalone paragraph \(archive\)](#). As recently as [11th September 2025](#) the following aggressive addition was absent:

*"Alaska Airlines may deny, revoke, or adjust Atmos Rewards points... if determined to have been granted in error, including due to system or partner issues, regardless of member fault."*

**"Due to system or partner issues"** - Alaska's own system flaws are no longer to be blamed.

**"Including after posted or redeemed"** - refunded miles can now be un-refunded.

**"Regardless of member fault"** - victims being blameless for account thefts is no longer a reason for reimbursement.

As recently as 11 September this paragraph was completely absent. This defensive legal firewall specifically relates to the ability to remove, or not replenish, loyalty points lost by a blameless member through system issues.

## Management Commentary

Press coverage of the phenomenon by [Fox13 Seattle](#) and [Kiro7](#) in July and the [Seattle Times](#) in November yielded only generic replies from Alaska and no meaningful engagement.

However Alaska VP of Loyalty announced on 7th October 2025 on Reddit that "fraud attempts are getting worse almost [daily](#)."

The 23rd June 2025 Hawaiian Airlines cyberattack's latest reference in [Q3 2025's 10Q](#) was:

\_"we do not believe the incident had ... a material impact ... The investigation remains active ... unable to determine the full impact [yet]" \_

After multiple IT outages that grounded flights, Alaska engaged Accenture on 31st October for a "comprehensive technology audit". Remarkably the incident was used as rationale to cancel, not postpone, the earnings call.

However the CFO provided the first commentary on the Accenture engagement on [4th December 2025](#)

"we don't have a systemic architecture failure... Have we just under-resourced ourselves? That's not what they [Accenture] found."

'Hygiene' and 'innovation' were cited as contributory factors to the outages:

*"...launched a brand new loyalty platform... and needed to make a lot of updates to our technology, our apps, our website"*

Notably the new platform's 20th August launch did nothing to inhibit the volume of loyalty points thefts in our collection of hacked accounts.

The direct response on IT infrastructure represents a *de facto* statement that compromised accounts are not a critical identified issue in the current audit.

## What Can and Cannot Be Concluded

**Established:** Amendment exists, protocol exists, timing correlates with incidents.

**Not established:** Whether senior management understood scale; whether amendment was specifically responsive to fraud.

The circumstantial pattern is suggestive. Management is best positioned to clarify.

---

# REGULATORY EXPOSURE

## Department of Transportation

Alaska's CEO personally signed a binding agreement with DOT on 14 September 2024 as a condition of the Hawaiian Airlines merger approval. [Section III.G.1.b](#) explicitly prohibits Alaska from taking actions that would "impose new limits on access, use, redemption, or validity" of miles.

### Alaska's practices appear to be inconsistent with this binding commitment:

1. **Telephone-only booking restrictions** imposed on breach victims constitute "new limits on access" - members must call during business hours (Monday-Saturday), wait average 100 minutes, and receive only one-hour account unlocks.
2. **"Regardless of member fault" revocation clause** added between 11 September and 29 November 2025 permits Alaska to "deny, revoke, or adjust points... due to system or partner issues, regardless of member fault" - directly authorising the devaluation the DOT agreement prohibits.

### Enforcement mechanisms available:

- 49 U.S.C. § 46301: Civil penalties up to \$37,377 per violation per day
- Agreement Section VI: DOT may pursue enforcement through federal court
- Each affected member constitutes a separate potential violation

## SEC (Financial Reporting)

- 10.40σ loyalty issuance anomaly unexplained in Q2 10-Q filing
- \$120M moved to non-current assets in Q3 with no disclosure of nature or collectibility
- \$58M retroactive reclassification in Q2 10-Q (post-spike) reduced apparent receivables increase from 159% to 74%

## Washington State Attorney General

- [RCW 19.255.010](#) requires breach notification within 30 days
  - Likely small proportion of 265 hacks announced, and attack vector indicates that would be a small proportion of total accounts
  - No public notifications identified
  - **Precedent:** Blackbaud multi-state settlement: \$49.5M
-

# FINANCIAL DEPENDENCY AND STRATEGIC RISK

## The Programme's Centrality

At Alaska Investor Day on 10 December 2024, management disclosed:

Metric	Value
Cash generated	\$2.2 billion+
Standalone programme valuation	\$12 billion+
Loyalty Programme Other Revenue	\$733 million

The \$2.2B cash figure attracts a margin we can estimate from its disclosures from Avianca (50% margin) and United (34% shown in 2020 Chapter 11). It likely delivers over \$1B of operating cash flow on total net profit of \$395 million

**The loyalty plan generates cash equivalent to the airline's total operations.**

## The \$2B Credit Facility

The loyalty plan secures a \$2B facility with Bank of America. Standard provisions include:

- Collateral maintenance requirements
- Material adverse change clauses

A 24x peer breach rate and functional disabling of online utility may constitute material impairment. Covenant implications cannot be assessed without facility documentation, but warrant investor attention.

## Strategic Risk Vectors

All these anomalies relate directly to this part of Alaska's business. Loyalty mile issuance, receivables from partners, members having miles stolen and accounts restricted.

**Accounting Integrity:** If the issuance-to-revenue ratio is broken, reported economics may not reflect reality.

**Partner Confidence:** The receivable non-collection raises questions about the Bank of America relationship.

**Customer Trust:** Victims are Alaska's best customers (high-balance accounts). Permanent restrictions degrade utility for members who generate the most value.

**Programme Currency:** A loyalty programme functions as private currency. Question marks on the integrity of the supply of loyalty points have repercussions on its value, just like real currencies.

## Ongoing Nature

These concerns are not historical. Incidents continue. 2FA remains unavailable. Each day without remediation accumulates additional exposure.

---

# CONCLUSION

## Summary of Findings

1. **10.40σ accounting anomaly** - unprecedented, unique among peers
2. **\$120M reclassified** without disclosure
3. **\$58M retroactive reclassification** characterised as "immaterial"
4. **26,500 estimated fraud victims** at 24x peer rate
5. **\$43M/\$45M convergence** between incident estimate and financial anomaly
6. **Terms amendment** shifting liability to customers

## Near-Term Catalysts

- Publication of this analysis
- Q4 2025 / FY2025 audit scrutiny (February 2026)
- Regulatory inquiry (SEC, DOT, Washington State AG)

## Management Response Requested (Specific Reconciliations)

1. Provide a rollforward of loyalty programme contract liabilities for Q2 2025 that separately quantifies: partner-sold point issuances, member-earned issuances, reinstatements/adjustments, breakage/estimate changes, and redemptions.
2. Provide a schedule of "Amounts due from affinity card partners" by counterparty and by aging/settlement timing (current vs >12 months), including cash receipts by quarter.
3. Provide a rollforward of "Other Non-Current Assets" between Q2 and Q3 2025 identifying the component(s) driving the \$120M increase, and whether any portion represents reclassified partner receivables/contract assets.
4. Explain the nature of the retroactive revision to 12/31/2024 affinity receivables, including: what was reclassified, why it was identified in Q2 (not during the annual audit), and the impact on comparability/trend.
5. State whether any material changes were made in Q2 2025 to loyalty programme SSP/breakage/fulfilment-cost estimates or to affinity partner contract terms, and quantify the income statement and balance sheet effect.

## Investment Conclusion

The accounting anomalies cannot be explained by commercial movements that do not merit disclosure. The cybersecurity crisis is undisclosed. The two phenomena correlate in timing and magnitude.

These concerns are not reflected in current valuation. Until management provides adequate explanation, Alaska Air Group shares face **material downside risk**.

---

**Appendices available separately:** Detailed accounting methodology, null hypothesis testing, incident documentation protocol, peer comparison data, regulatory framework reference, and complete data book with SEC filing extracts.

---

## ABOUT THE AUTHOR

Tommy Caton was co-founder, Chief Revenue Officer, and Chief Financial Officer of travel data analytics firm AirDNA from 2015 to 2022. He holds an MBA from the Kellogg School of Management (Northwestern University) and worked for four years in KPMG's Corporate Finance division. This report is all his own work.

The author is not a professional short seller. This analysis originated from noticing irregularities in publicly available information, which led to taking a short position in Alaska Air Group. Prior to this, the author's portfolio consists predominantly (95%) of diversified funds and just one individual stock.

[tommy@noseyparker.org](mailto:tommy@noseyparker.org)

# APPENDIX A: DETAILED ACCOUNTING METHODOLOGY

## A.1 Issuance-to-Revenue Ratio Calculation

This ratio is a useful analytical proxy for the underlying economics of the loyalty programme under ASC 606. It is not a metric defined or required by the standard itself.

The ratio is calculated as:

**Ratio = Increase in liability for loyalty points issued (quarterly) / Loyalty Programme Other Revenue (quarterly)**

Data is extracted from Alaska Air Group 10-Q and 10-K filings, specifically:

- "Increase in liability for loyalty points issued" from Note 3: Revenue
- "Loyalty programme other revenue" from segment revenue disclosures

Quarterly figures for cumulative YTD disclosures are derived by subtracting prior quarter YTD figures.

## A.2 Baseline Period Selection

The baseline period (Q3 2022 through Q1 2025) was selected based on: availability of consistent disclosure format post-ASC 606 implementation; exclusion of pandemic-affected periods; inclusion of sufficient observations for statistical validity (n=11); and termination before the anomaly quarter.

## A.3 Statistical Analysis

**Z-Score Calculation:**

$$Z = (X - \mu) / \sigma$$

Where:

- X = Observed Q2 2025 ratio (2.743)
- $\mu$  = Baseline mean (1.8836)
- $\sigma$  = Baseline standard deviation (0.0826)

$$Z = (2.743 - 1.8836) / 0.0826 = 10.40$$

### Sensitivity Analysis:

Baseline Period	Quarters (n)	Mean ( $\mu$ )	Std Dev ( $\sigma$ )	Q2 2025 Z-Score
Q3 2022 - Q1 2025	11	1.8836	0.0826	10.40 $\sigma$
Q1 2024 - Q1 2025	5	1.918	0.101	8.14 $\sigma$
Q1 2022 - Q1 2025	13	1.875	0.115	7.50 $\sigma$

All specifications yield Z-scores exceeding 7 $\sigma$ . The finding is robust to baseline selection.

### A.4 Peer Comparison Methodology

Quarterly issuance-to-revenue ratios were calculated for United Airlines (UAL), Delta Air Lines (DAL), and American Airlines (AAL) using identical methodology applied to their respective SEC filings.

#### Baseline Statistics (Q3 2022 - Q1 2025):

Airline	Mean ( $\mu$ )	Std Dev ( $\sigma$ )	Coefficient of Variation
Alaska	1.8836	0.0826	4.4%
United	1.200	0.094	7.8%
Delta	1.360	0.064	4.7%
American	1.358	0.375	27.6%

## A.5 Balance Sheet Movements

### Affinity Card Receivables:

Period	Affinity Receivables (\$M)	Q-o-Q Change	% Change
Q1 2025	111	-65	-37%
<b>Q2 2025</b>	<b>306</b>	<b>+195</b>	<b>+176%</b>
Q3 2025	177	-129	-42%

### Other Noncurrent Assets:

Period	Other Noncurrent Assets (\$M)	Q-o-Q Change	% Change
Q2 2025	316	-	-
Q3 2025	436	+120	+38%

### Cash Flow Corroboration:

The Q2 2025 cash flow statement shows a use of operating cash of approximately \$171M for accounts receivable movements, confirming the receivables spike was non-cash in nature. The subsequent Q3 2025 receivables decline did not generate corresponding operating cash inflow, supporting the inference that the asset was reclassified rather than collected.

## A.6 Partner-to-Passenger Redemption Ratio Methodology

The partner-to-passenger redemption ratio provides a merger-normalised metric for assessing whether partner redemptions are elevated relative to overall redemption activity.

### Ratio Calculation:

Ratio = Loyalty redemptions - Partner Airlines (quarterly) / Loyalty redemptions - Passenger Revenue (quarterly)

### Rationale:

Both partner and passenger redemptions should scale proportionally with the merged entity's larger membership base. If the Hawaiian merger simply added Hawaiian's loyalty economics to

Alaska's, the ratio should remain stable. Deviations from the historical ratio therefore indicate changes in the composition of redemptions rather than mere scale effects from the merger.

**Baseline Statistics (Q1 2024 - Q1 2025):**

Measure	Value
Mean ( $\mu$ )	0.145
Standard deviation ( $\sigma$ )	0.019
Range	0.120 - 0.168

**Post-Baseline Observations:**

Quarter	Ratio	Z-Score
Q2 2025	0.201	+2.95 $\sigma$
Q3 2025	0.222	+4.05 $\sigma$

The Q3 2025 deviation of 4.05 standard deviations has a probability of less than 0.005% under normal distributional assumptions.

**A.7 Limitations**

This analysis was conducted using publicly available SEC filings. The following information was not available and would be required for definitive conclusions: internal accounting memoranda and judgement documentation; Bank of America contract terms and amendments; detailed composition of Other Noncurrent Assets; partner compensation expense detail by carrier; and management explanations for observed patterns.

A comprehensive forensic audit with management access would be required to definitively determine the cause and precise magnitude of the patterns identified. Management may have information and rationales not apparent from public disclosures that differ from the interpretations presented here.

**A.8 Null Hypothesis Exploration**

Before concluding that the Q2-Q3 2025 accounting patterns warrant concern, a responsible analysis must consider whether benign explanations could account for the observations. This section examines 17 alternative hypotheses that might be offered to explain the 10.40 $\sigma$  statistical anomaly, the \$195M receivables spike, and the subsequent \$120M reclassification to

noncurrent assets. Each hypothesis is assessed against what the numbers would need to show if true, and what GAAP would require to be disclosed.

The framework applied to each hypothesis is straightforward: if a benign explanation is correct, it must be consistent with the quantitative data, temporally plausible, and accompanied by the disclosures that GAAP requires for material transactions of that nature. Failure on any criterion suggests the explanation is inadequate.

---

## Hypothesis 1: Hawaiian Airlines Integration Accounting

### **The Benign Explanation**

The Hawaiian Airlines acquisition closed on 18 September 2024. Complex acquisitions involve purchase price allocations, fair value adjustments, and measurement period refinements under ASC 805. An observer might reasonably assume that the Q2 2025 loyalty programme anomalies reflect integration accounting noise from absorbing Hawaiian's HawaiianMiles programme.

### **What Would Need to Be True**

If integration accounting caused the Q2 2025 anomaly, the following signatures would be expected. The loyalty programme ratio deviations would have appeared immediately after the September 2024 acquisition close, or at least shown a gradual trend through Q4 2024 and Q1 2025 as integration progressed. Any measurement period adjustments affecting loyalty accounting would be disclosed in Note 2 (Business Combinations), as required by ASC 805-10-50-2(h). The MD&A would explain integration impacts on loyalty programme other revenue and related balance sheet items.

### **Why It Fails**

The timing is inconsistent with an integration explanation. Q4 2024 and Q1 2025 ratios were 2.02 and 2.00 respectively, both within normal ranges and showing no anomaly. The  $10.40\sigma$  deviation appeared only in Q2 2025, eight months after the acquisition closed, then immediately reverted to 1.87 in Q3 2025. This single-quarter spike followed by complete normalisation is inconsistent with gradual integration effects.

The filing states that no material ASC 805 measurement period adjustments were recorded during the quarter. This limits the plausibility of a late purchase accounting true up as the driver of the observed anomaly. It does not, however, preclude post close operational integration effects, such as programme harmonisation, award chart changes, partner settlement mechanics, IT migrations, or customer conversion incentives. If Hawaiian integration is the explanation, it would therefore need to operate through such operational mechanisms rather

than through purchase accounting adjustments, and would still be expected to support a coherent commercial and accounting narrative if material.

**GAAP Reference:** ASC 805-10-50-2(h) requires disclosure of material effects of acquisitions on reported results. No such disclosure links the Q2 2025 anomaly to Hawaiian integration.

**Verdict:** ASC 805 measurement period accounting does not explain a one quarter, isolated  $10.40\sigma$  event appearing eight months after acquisition close; any integration based explanation would need to be operational in nature and should still support a coherent disclosed narrative if material.

---

## Hypothesis 2: Standalone Selling Price Volatility

### The Benign Explanation

Under ASC 606, Alaska must allocate the cash received from Bank of America between a marketing component (recognised immediately as revenue) and a transportation component (deferred until miles are redeemed). This allocation depends on the estimated standalone selling price (SSP) of the transportation element. An observer might suggest that Alaska refined its SSP estimate in Q2 2025, causing more of each dollar received to be allocated to deferred revenue rather than immediate recognition.

### What Would Need to Be True

The issuance to revenue ratio is an analytical proxy rather than a direct accounting metric. If one assumes, illustratively, that the observed ratio movement were driven primarily by changes in allocation economics such as SSP, the implied change would be very large by industry standards. However, the ratio can also be affected by mix effects, classification timing, and changes in partner economics. Accordingly, the implied percentage should be interpreted as an order of magnitude indicator rather than a precise inferred SSP revision.

### Why It Fails

No disclosure of any SSP or breakage assumption change appears in the Q2 2025 10-Q. Alaska's 2024 10-K provides sensitivity analysis on key loyalty assumptions, but no Q2 2025 update references any change. The implied magnitude of any SSP shift, if one assumes allocation economics are the primary driver of the proxy movement, would be exceptionally large by industry standards. However, because the ratio can be influenced by mix, timing, classification, and partner economics, the proxy cannot be reverse engineered into a single precise SSP percentage change with confidence.

Furthermore, if Alaska genuinely changed its SSP estimate by this magnitude without disclosure, that would itself constitute a GAAP violation under ASC 606-10-50-17. The

hypothesis thus fails the "GAAP trap": either no material change occurred (leaving the anomaly unexplained), or a material change occurred without required disclosure (constituting a compliance failure).

**GAAP Reference:** ASC 606 10 50 17 through 50 20 require disclosure of the significant judgements, and changes in judgements, that affect the determination of the amount and timing of revenue recognition. While the Codification does not require registrants to restate or highlight every quarterly change in judgement, a material change in SSP, breakage assumptions, or other key loyalty programme judgements that materially affects reported results would ordinarily be explained in the interim period narrative disclosures.

**Verdict:** SSP volatility fails both quantitative plausibility (35-40% single-quarter shift is economically implausible) and the disclosure test (no change was disclosed).

---

### Hypothesis 3: Bank of America Contract Restructuring

#### The Benign Explanation

Alaska's Mileage Plan generates most of its loyalty revenue through its co-branded credit card partnership with Bank of America. An observer might suggest that Q2 2025 reflected a contract restructuring with Bank of America, perhaps a pre-payment arrangement, modified pricing structure, or advance purchase of miles ahead of a new card product launch.

#### What Would Need to Be True

ASC 606 does not require registrants to label or separately disclose every contract modification. However, the standard requires sufficient disclosure to enable users to understand the nature, amount, timing, and uncertainty of revenue and cash flows. A material change in commercial terms affecting loyalty economics would ordinarily be expected to be explainable through the ASC 606 disclosure framework, including disclosures about performance obligations, significant payment terms, contract balances, and significant judgements. Where such a change materially affects an interim period, a registrant would typically provide narrative explanation in its quarterly filing even if the Codification does not prescribe a discrete "contract modification" disclosure.

#### Why It Fails

The temporal sequence is inconsistent. The Q2 2025 anomaly occurred in April-June 2025. Alaska's disclosed Bank of America contract amendments occurred in September 2025, and the Summit Visa Infinite card launched in August 2025, both subsequent to the anomaly quarter. Contractual modifications cannot retroactively cause accounting effects in prior quarters.

Moreover, the cash flow statement does not show unusual cash receipts in Q2 2025 that would correspond to a prepayment. The receivables increase of \$195M represents the opposite of a prepayment, as it suggests amounts owed to Alaska rather than advance cash received.

**GAAP Reference:** ASC 606-10-50-12 requires disclosure of significant contract modifications.

**Verdict:** Contract restructuring is temporally impossible as disclosed amendments post-date the anomaly, and the cash flow pattern contradicts any prepayment hypothesis.

---

## Hypothesis 4: Breakage Assumption Refinement

### The Benign Explanation

Airlines estimate the proportion of issued miles that will ultimately expire unredeemed (breakage). If Alaska reduced its breakage estimate in Q2 2025, expecting more miles to be redeemed, it would defer more revenue and increase the loyalty liability. An observer might suggest this explains the elevated issuance-to-revenue ratio.

### What Would Need to Be True

Using management's disclosed annual breakage sensitivity as a reference point, an illustrative back of the envelope analysis suggests that a very large change in breakage assumptions would be required to produce a liability movement of the magnitude observed in a single quarter. This estimate assumes a broadly linear relationship between breakage rate changes and liability impact, which may not hold precisely in practice. The conclusion is therefore directional: any such breakage revision would need to be unusually large relative to historical practice.

### Why It Fails

ASC 250-10-50-4 explicitly requires disclosure of material changes in accounting estimates. No such disclosure appears. Alaska's Q2 2025 10-Q makes no mention of breakage assumption changes. If a 15 percentage point breakage revision occurred without disclosure, that would itself be a GAAP violation.

Additionally, the single-quarter spike and immediate reversion pattern is inconsistent with a genuine breakage assumption change. If Alaska genuinely believed more miles would be redeemed, that belief would persist across quarters rather than appearing and disappearing within 90 days.

**GAAP Reference:** ASC 606 requires disclosures sufficient to enable users to understand the nature, amount, timing, and uncertainty of revenue and cash flows, including disclosure of significant judgements and explanations of material movements in contract balances. Material

contract modifications would ordinarily be expected to be explainable within that disclosure framework and, where material to the interim period, discussed in the quarterly narrative.

**Verdict:** Breakage refinement fails the GAAP disclosure trap, as either no material change occurred (anomaly unexplained), or a material change occurred without disclosure (GAAP violation). The required magnitude is also economically implausible.

---

## Hypothesis 5: Industry-Wide Disruption

### The Benign Explanation

External factors such as changes in consumer credit card spending behaviour, macroeconomic shifts, or regulatory changes affecting frequent flyer programmes might have caused unusual patterns across the airline industry in Q2 2025. An observer might suggest Alaska is simply reflecting broader industry trends.

### What Would Need to Be True

If industry-wide factors caused the anomaly, peer airlines would exhibit similar deviations from their historical patterns. United, Delta, and American, all operating large co-branded credit card programmes with similar structures, would show comparable ratio movements.

### Why It Fails

Peer comparison demonstrates the anomaly is unique to Alaska.

Airline	Q2 2025 Ratio	Baseline Mean	Z-Score
Alaska	2.74	1.88	+10.40σ
United	1.20	1.20	0.00σ
Delta	1.44	1.36	+1.25σ
American	1.18	1.36	-0.46σ

United's ratio was precisely at its baseline mean. Delta showed only modest elevation. American was actually below its historical average. Whatever occurred at Alaska in Q2 2025 has no parallel at major US peers during the same period.

**GAAP Reference:** No specific provision; this is a factual test of whether the anomaly reflects company-specific versus industry-wide factors.

**Verdict:** Industry-wide disruption is empirically rejected. The anomaly is Alaska-specific.

---

## Hypothesis 6: Summit Card Pre-Positioning

### The Benign Explanation

Alaska launched its Summit Visa Infinite premium credit card in August 2025. An observer might suggest that Bank of America pre-purchased miles in Q2 2025 in anticipation of this launch, causing the issuance spike.

### What Would Need to Be True

If Bank of America pre-positioned miles for Summit, the purchase would generate marketing revenue recognition under ASC 606. Marketing revenue, which is recognised immediately upon mile delivery, would show substantial year-on-year growth in Q2 2025.

### Why It Fails

The decomposition of loyalty programme other revenue reveals that marketing and brand revenue grew only 4% year-on-year in Q2 2025, rising from approximately \$135M to \$140M. This modest growth is inconsistent with a substantial mile pre-purchase. The \$181M excess issuance implied by the ratio anomaly vastly exceeds the \$5M year-on-year growth in the marketing component.

Furthermore, the Summit card launched in Q3 2025, by which point the ratio had already normalised. If pre-positioning occurred, its effects would logically persist through the launch quarter rather than reversing before the card even became available.

**GAAP Reference:** ASC 606 requires revenue recognition when performance obligations are satisfied. Mile delivery triggers immediate marketing revenue recognition.

**Verdict:** Summit pre-positioning fails the marketing revenue test, as the relevant revenue line did not grow commensurately with the issuance spike.

---

## Hypothesis 7: Receivable Timing and Cash Collection Lag

### The Benign Explanation

Trade receivables fluctuate based on billing cycles and payment terms. An observer might suggest the \$195M Q2 2025 receivables increase simply reflects timing of Bank of America payments, and that Q3 2025 saw normal cash collection.

## What Would Need to Be True

If the receivables increase were genuine and subsequently collected, the Q3 2025 cash flow statement would show corresponding operating cash inflow. The receivables decline would be matched by cash receipts, and the asset would not need to be reclassified elsewhere on the balance sheet.

## Why It Fails

The cash flow statement tells a different story. The Q2 2025 cash flow statement shows a use of operating cash of approximately \$171M for accounts receivable movements, confirming the receivables spike was non-cash in nature. The Q2 2025 cash flow statement reflects a material operating cash outflow associated with accounts receivable movements, consistent with the receivables spike being largely non cash in nature. In Q3 2025, the reduction in reported receivables is not mirrored by an equally clear, isolated operating cash inflow attributable to collections. This pattern is consistent with some form of reclassification, netting, or offset within working capital rather than straightforward cash settlement, but the financial statements do not provide sufficient disaggregation to conclude definitively.

However, for a \$129M receivable decline to reflect cash collection without being visible as a material operating cash tailwind, other working-capital items would need to show an equal-and-opposite outflow of comparable magnitude in the same quarter. A working-capital bridge can therefore falsify (or corroborate) this defence even without counterparty-level cash disclosure.

Instead of cash collection, approximately \$120M appears to have been reclassified from current receivables to Other Noncurrent Assets, which rose from \$316M to \$436M between Q2 and Q3 2025. This reclassification received no explanatory disclosure.

**GAAP Reference:** ASC 210-10-45-1 governs balance sheet classification and requires assets to be classified based on their nature and expected realisation. Regulation S-K Item 303 requires MD&A disclosure of material changes in liquidity. If collectibility became uncertain or terms were modified in a manner that changes risk, the company would be expected to assess and reflect expected credit losses and describe the nature of the receivable/contract asset and collection assumptions.

**Verdict:** The cash flow data contradict the timing explanation. The receivable was not collected; it was apparently reclassified without disclosure.

---

Hypothesis 8: Reclassification to Noncurrent Receivable Due to Extended Payment Terms

## The Benign Explanation

Bank of America might have negotiated extended payment terms on a portion of its obligations to Alaska. An observer might suggest the movement from current receivables to noncurrent assets reflects a straightforward reclassification of the same receivable based on longer expected collection timing.

### **What Would Need to Be True**

If Bank of America payment terms extended beyond one year, the receivable would remain a receivable, properly classified as noncurrent. ASC 606-10-45-3 is clear that a receivable is an unconditional right to consideration. If the right remains unconditional but simply has a longer collection horizon, it would be presented as a noncurrent receivable with appropriate disclosure. If a significant financing component exists due to the extended terms, ASC 606-10-32-15 requires either interest income or contra-revenue treatment. MD&A would address the liquidity implications of a major customer extending payment terms.

### **Why It Fails**

The asset did not move to a "noncurrent receivables" line. It moved into the generic "Other Noncurrent Assets" category, which is not a receivable classification. There is no disclosure of modified Bank of America payment terms. There is no discussion of significant financing components or interest income. MD&A makes no mention of any impact on liquidity or working capital from modified partner payment terms.

For a movement of this magnitude, roughly \$120M affecting a significant business relationship, silence in the financial statement notes and MD&A is inconsistent with standard disclosure practices.

**GAAP Reference:** ASC 606 distinguishes contract assets from receivables based on whether the entity's right to consideration is conditional on something other than the passage of time. Where the entity has an unconditional right to consideration, the balance is presented as a receivable. Where consideration remains conditional on future performance or other factors, the balance is presented as a contract asset. Reclassification between these categories therefore reflects a change in the nature of the underlying right, not merely a balance sheet relabelling. As stated in the previous hypothesis, the company would be expected to assess and reflect expected credit losses and describe their nature.

**Verdict:** The "longer terms" explanation fails on classification (not presented as a receivable), financing treatment (no interest disclosed), and liquidity disclosure (no MD&A mention).

---

## Hypothesis 9: Contract Asset Rather Than Receivable Relabelling

### **The Benign Explanation**

ASC 606 distinguishes between receivables (unconditional rights) and contract assets (conditional rights, dependent on further performance). An observer might suggest the issue is merely one of labelling, that what Alaska calls a "receivable" is actually a contract asset, and the subsequent movement reflects proper reclassification.

### **What Would Need to Be True**

If the amounts were truly contract assets, they would be presented and described as such under ASC 606-10-45-3. Note 3 (Revenue Recognition) would discuss contract asset balances, movements, and the nature of the conditionality. Any reclassification from receivable to contract asset would be explained, including what performance triggers must be satisfied.

### **Why It Fails**

Alaska's Q2 2025 10-Q explicitly presents "amounts due from affinity card partners and from other partners" as receivables, not contract assets. The presentation treats these as unconditional rights to consideration. In Q3 2025, the amounts do not appear in a contract asset line; instead, they apparently move into generic "Other Noncurrent Assets" with no contract asset disclosure.

There is no explanation of what conditionality or performance triggers would apply. The company treated these as receivables (unconditional), then moved a portion to an opaque balance sheet category without following ASC 606 contract asset disclosure requirements.

**GAAP Reference:** ASC 606-10-45-3 distinguishes receivables from contract assets based on conditionality. ASC 606-10-50-8 requires disclosure of contract balance explanations.

**Verdict:** This is not a mere labelling issue. The company treated these as receivables, then obscured part of them without following contract asset disclosure rules.

---

## Hypothesis 10: Immaterial Presentation Differences

### **The Benign Explanation**

Management characterised the \$58M retroactive restatement of 2024 affinity receivables as "immaterial." An observer might extrapolate this characterisation to the broader pattern, suggesting the entire Q2-Q3 2025 sequence represents nothing more than immaterial presentation adjustments not warranting detailed disclosure.

### **What Would Need to Be True**

For the "immaterial" characterisation to hold across the full pattern, the amounts involved would need to be quantitatively and qualitatively immaterial under SEC Staff Accounting Bulletin 99 (SAB 99). SAB 99 establishes that materiality is not purely a numerical threshold; qualitative factors matter equally. An item is material if "there is a substantial likelihood that a reasonable investor would consider it important."

### **Why It Fails**

The quantitative test fails decisively. The estimated misstatement range of \$120M to \$200M represents 30% to 51% of Alaska's 2024 net income of \$395M. Even the most conservative estimate exceeds the commonly applied 5% threshold by a factor of six. The \$58M restatement alone, at 15% of net income, strains any reasonable definition of immateriality.

The qualitative factors under SAB 99 are equally problematic. The anomaly masks a key revenue trend in Alaska's third-largest revenue category. The reclassification distorts working capital and liquidity metrics used by investors. The pattern exhibits an exact temporal correlation with an extreme statistical outlier. The anomaly is unique to Alaska among peer airlines, suggesting company-specific factors rather than industry dynamics. The Bank of America relationship is explicitly described as a strategic asset in investor materials.

By any reasonable standard, these are not immaterial presentation differences.

**GAAP Reference:** SAB 99 sets forth qualitative factors for materiality assessment beyond numerical thresholds.

**Verdict:** "Presentation only" is not credible at these magnitudes. The amounts exceed standard materiality thresholds by 6-10x, and multiple SAB 99 qualitative factors are triggered.

---

## Hypothesis 11: One-for-One Hawaiian Point Conversion Funded by Affinity Partner Economics

### **Benign Explanation**

Following the Hawaiian Airlines acquisition, Alaska made a post-close commercial decision to convert HawaiianMiles into Alaska miles on a one-for-one basis. If HawaiianMiles historically carried lower standalone selling prices or lower expected fulfilment costs than Alaska miles, this conversion would increase the economic value of the outstanding loyalty obligation. Under this hypothesis, the Q2 2025 increase in loyalty contract liabilities reflects a cumulative catch-up to align the converted Hawaiian member population with Alaska programme economics. Rather than recognising the offset through a reduction in loyalty programme other revenue, Alaska recognised a receivable from its affinity card partner on the basis that the incremental obligation would be contractually funded by the partner over time.

## What Would Need to Be True

- The one-for-one conversion decision occurred post-close and was not an acquisition-date fact, such that the accounting impact properly falls under ASC 606 rather than ASC 805 purchase accounting.
- The conversion materially increased the value of outstanding points, requiring recognition of an incremental loyalty contract liability via a change in estimate or contract modification analysis.
- The affinity card agreement includes provisions that obligate the partner to fund the increased value of previously issued points, giving Alaska a present and enforceable right to incremental consideration.
- The recognised balance qualifies as a receivable rather than a contract asset, meaning the right to consideration is unconditional or conditional only on the passage of time.
- Any portion expected to be collected beyond twelve months is appropriately classified as non-current with clear disclosure of settlement terms.

## Why It Likely Fails

This hypothesis requires a combination of a post-close economic upgrade and a contractual repricing of the affinity relationship, neither of which is described in the public filings. The filings do not disclose a material change in loyalty programme economics, a repricing or true-up mechanism with the affinity partner, or a renegotiation of partner funding terms. The subsequent reclassification of the balance into a generic “Other Non-Current Assets” line item, rather than a clearly identified receivable or contract asset with disclosed terms, is inconsistent with how material, enforceable partner claims are typically presented.

**GAAP Reference:** ASC 606 requires receivables to reflect unconditional rights to consideration and contract assets to reflect rights conditional on future performance or events. Material changes in revenue recognition judgements or contract balances are expected to be explainable through disclosure. Post-acquisition changes in loyalty economics do not adjust goodwill and are accounted for through revenue recognition mechanics rather than purchase accounting.

**Verdict:** A one-for-one conversion can explain an increase in loyalty contract liabilities in principle. It does not naturally explain recognition of a large affinity receivable unless the partner is contractually obligated to fund the incremental value. Absent disclosure of such contractual mechanisms, this hypothesis remains incomplete.

---

Hypothesis 12: Single Loyalty Platform Migration Revaluation of Acquired Mileage Liabilities

## Benign Explanation

The Q2 2025 anomaly reflects a non-cash technical remeasurement when HawaiianMiles balances were migrated onto Alaska's loyalty platform and subledger. HawaiianMiles points were historically measured using Hawaiian's assumptions. Upon migration, Alaska aligned the acquired outstanding miles to Alaska's higher SSP and redemption cost assumptions, producing a one-time increase in the loyalty contract liability without corresponding revenue.

### **What Would Need to Be True**

- The migration occurred in Q2 2025 and required formal alignment of valuation and recognition policies.
- HawaiianMiles liabilities were carried under materially different assumptions that, when aligned, increased the measured obligation.
- The adjustment reflects either acquisition-date facts finalised within the ASC 805 measurement period or a post-close change in estimate under ASC 606.
- If ASC 805 applies, goodwill would increase. If ASC 606 applies, a cumulative catch-up to revenue would occur.
- The migration explains a discrete step change rather than a gradual trend.

### **Why It Likely Fails**

If the adjustment were an ASC 805 measurement period update, goodwill would be affected and disclosed as such. If it were an ASC 606 change in estimate, a visible revenue impact would be expected. The filings show neither a material goodwill adjustment nor a commensurate revenue catch-up, and provide no narrative explaining a migration-driven revaluation of this magnitude.

**GAAP Reference:** ASC 805 measurement period adjustments adjust goodwill for acquisition-date facts. ASC 606 changes in estimate affecting loyalty obligations require cumulative catch-up accounting through revenue unless funded by a third party.

**Verdict:** A platform migration can trigger a liability remeasurement, but the accounting must resolve through either goodwill or revenue. The absence of either outcome weakens this explanation.

---

## Hypothesis 13: Long-Term Affinity Partner Financing Structure

### **Benign Explanation**

The Q2 2025 spike in receivables reflects recognition of a claim against the affinity card partner to fund integration-related loyalty costs, with the Q3 reclassification to non-current assets reflecting formalisation of a long-term settlement schedule extending beyond twelve months.

### **What Would Need to Be True**

- The affinity agreement includes enforceable provisions requiring the partner to fund integration or loyalty harmonisation costs.
- Alaska has an unconditional or time-only conditional right to the consideration.
- The timing of expected cash flows supports non-current classification.
- Any significant financing component is appropriately considered and disclosed.
- The arrangement is sufficiently material to warrant explanation.

### **Why It Likely Fails**

The filings do not describe a material renegotiation or repricing of the affinity agreement, nor do they clearly present the balance as a non-current receivable or contract asset with disclosed terms. Presentation within a generic non-current asset category obscures the nature of the claim and is inconsistent with standard practice for material partner financing arrangements.

**GAAP Reference:** ASC 606 distinguishes receivables from contract assets based on unconditional rights to consideration. Material partner arrangements and long-dated settlement terms are expected to be disclosed.

**Verdict:** A long-term partner funding arrangement could explain the classification change, but the absence of disclosure and clear presentation materially undermines this hypothesis.

---

## Hypothesis 14: Post-Migration Redemption Surge from Newly Enabled Partner Access

### **Benign Explanation**

The elevated partner redemption costs reflect legitimate pent-up demand by Hawaiian members gaining access to Alaska's broader partner network following platform integration, rather than fraud or cybersecurity failures.

### **What Would Need to Be True**

- Platform integration materially expanded partner redemption options.
- Hawaiian members redeemed at higher-value partners at elevated rates.
- Redemption mix shifted materially toward higher-cost partners.
- Customer complaints reflect migration friction rather than account compromise.

### **Why It Likely Fails**

While this hypothesis plausibly explains increased redemption costs and customer noise, it does not explain a discrete, large increase in loyalty contract liabilities. A redemption surge reduces liabilities rather than creates them, unless paired with a separate liability revaluation event that is not clearly disclosed.

**GAAP Reference:** Under ASC 606, redemptions reduce contract liabilities and trigger cost recognition. Redemption activity alone does not increase deferred revenue.

**Verdict:** Redemption surges explain cost pressure and customer disruption, but not the observed liability issuance anomaly in isolation.

---

## Hypothesis 15: Measurement Period Adjustments Under ASC 805

### Benign Explanation

The \$58 million retroactive adjustment reflects a standard ASC 805 measurement period refinement to acquired balances, such as legacy Hawaiian receivables, and is not indicative of error or irregularity.

### What Would Need to Be True

- The adjustment relates to acquisition-date facts.
- It falls within the one-year measurement period.
- The adjustment affects goodwill rather than current-period earnings.
- The nature of the adjustment is described in the purchase accounting disclosures.

### Why It Likely Fails

Measurement period adjustments can explain retrospective changes, but they do not explain a Q2 2025 loyalty issuance-to-revenue ratio spike unless the spike itself reflects a purchase accounting adjustment. The filings indicate no material measurement period adjustments to the loyalty obligation, limiting the explanatory power of this hypothesis.

**GAAP Reference:** ASC 805 permits retrospective adjustment of provisional amounts for acquisition-date facts, with corresponding goodwill adjustments.

**Verdict:** Measurement period accounting can explain discrete retrospective changes, but it does not plausibly explain the full Q2–Q3 2025 pattern observed.

## Hypothesis 16: Mass Reinstatements / Customer Make-Goods (Issuance Without Consideration)

### The Benign Explanation

Alaska reinstated large volumes of previously issued miles (or granted customer make-good credits) due to account compromise, operational correction, or migration issues. This would increase “liability for loyalty points issued” without increasing “loyalty programme other revenue.”

## What Would Need to Be True

- The reinstated/credited miles were recorded as an increase to the loyalty contract liability in Q2 2025.
- The offset was recorded as (i) an operating expense (customer service/fraud), or (ii) contra-revenue within passenger or loyalty revenue, or (iii) another clearly identifiable income statement line.
- The scale would be reconcilable to a discrete event and explain the reversion in Q3.
- If driven by cyber compromise, risk/incident disclosure would be expected to align with the magnitude of customer restitution.

## Why It Fails

Public disclosures do not identify a discrete income statement line item consistent with a customer restitution event of the magnitude implied by the \$180M “excess” liability creation, nor do they provide a quantified rollforward that isolates reinstatements/adjustments versus partner-funded issuances.

**GAAP Reference:** ASC 606 requires contract liability movements to be explainable through contract balance disclosures; material changes in judgments and material movements that affect revenue timing should be understandable from disclosures.

**Verdict:** Reinstatements can explain the *direction* of the ratio move but fail the disclosure and reconciliation test absent quantified rollforwards and identifiable offsets.

## Hypothesis 17: Revenue Caption Reclassification (Denominator Shift)

### The Benign Explanation

The observed issuance-to-revenue ratio spike is not driven by changes in loyalty issuance economics, but by a temporary reclassification of loyalty-related revenue between “Loyalty programme other revenue” and other revenue captions (for example passenger revenue or marketing revenue). Under this explanation, the denominator of the ratio was understated in Q2 2025 due to presentation choices rather than economic change.

## What Would Need to Be True

For this explanation to hold, the following conditions would need to be met:

- Alaska reclassified a material portion of loyalty-related consideration away from “Loyalty programme other revenue” in Q2 2025.

- The reclassification affected only the presentation of revenue, not total revenue, and therefore did not trigger changes in cash flow.
- Comparative periods were either recast, or the reclassification was disclosed clearly enough for investors to understand period-to-period comparability.
- The reclassification reversed or normalised in Q3 2025, coinciding with the ratio's reversion to baseline.

## Why It Fails

No disclosure in the Q2 2025 or Q3 2025 filings describes any reclassification of loyalty-related revenue captions. There is no footnote explaining a change in revenue presentation, no recast of prior-period comparatives, and no MD&A discussion of revenue classification changes affecting trend analysis.

Absent disclosure, investors have no basis to conclude that the ratio spike reflects a denominator artefact rather than a genuine economic or accounting event. Moreover, a reclassification large enough to produce a  $10.40\sigma$  deviation would be qualitatively material under SAB 99 and would ordinarily be disclosed even if total revenue were unchanged.

**GAAP Reference:** ASC 606-10-50 and Regulation S-K Item 303 require disclosure sufficient to enable users to understand the nature and comparability of revenue streams. Material changes in revenue presentation that affect trend analysis require explanation.

**Verdict:** A revenue caption reclassification could, in theory, distort the issuance-to-revenue ratio without changing underlying economics. In practice, the absence of any disclosure or comparative recast renders this explanation unsupported by the public filings.

---

## Summary of Null Hypothesis Evaluation

This analysis examined seventeen potential benign explanations for the Q2–Q3 2025 accounting patterns observed at Alaska Air Group. Each hypothesis was evaluated against three criteria:

1. Quantitative sufficiency to explain the magnitude of the observed movements.
2. Temporal alignment with the discrete, one-quarter nature of the anomaly.
3. Consistency with the disclosure and presentation requirements of U.S. GAAP.

Hypothesis	Quantitative	Temporal	Disclosure	Verdict
Hawaiian Integration (ASC 805)	Fail	Fail	Fail	Rejected

<b>Hypothesis</b>	<b>Quantitative</b>	<b>Temporal</b>	<b>Disclosure</b>	<b>Verdict</b>
SSP Volatility	Fail	Pass	Fail	Rejected
Contract Restructuring	N/A	Fail	Fail	Rejected
Breakage Refinement	Fail	Pass	Fail	Rejected
Industry-Wide Disruption	Fail	N/A	N/A	Rejected
Summit Pre-Positioning	Fail	Fail	N/A	Rejected
Receivable Timing	Fail	Fail	N/A	Rejected
Extended Payment Terms	N/A	Pass	Fail	Rejected
Contract Asset Relabelling	N/A	Pass	Fail	Rejected
Immaterial Presentation	Fail	N/A	Fail	Rejected
One-for-One Hawaiian Conversion	Fail	Pass	Fail	Rejected
Platform Migration Revaluation	Fail	Fail	Fail	Rejected
Long-Term Partner Financing	Pass	Pass	Fail	Rejected
Post-Migration Redemption Surge	Fail	Pass	N/A	Rejected

Hypothesis	Quantitative	Temporal	Disclosure	Verdict
Measurement Period Adjustments	Fail	Fail	Pass	Rejected
Mass Reinstatements / Make-goods	Pass	Pass	Fail	Rejected
Revenue Caption Reclassification	N/A	Pass	Fail	Rejected

Across all seventeen hypotheses, the same structural constraint applies. Any benign explanation capable of producing the observed Q2–Q3 2025 patterns must simultaneously satisfy magnitude, timing, and disclosure requirements. No hypothesis satisfies all three.

Where an explanation can account for the magnitude, it fails on timing or disclosure. Where it aligns temporally, it lacks quantitative sufficiency or requires accounting effects that are not visible in the financial statements.

This creates a consistent GAAP constraint: either the benign explanation is incorrect, leaving the anomaly unexplained, or it is correct but would have required disclosure that is absent. Both outcomes converge on the same conclusion: the Q2–Q3 2025 accounting patterns warrant explanation that has not been provided in the public filings.

## A.9 Accounting Signatures: Expected Financial Statement Effects by Hypothesis

The table below summarises the accounting signatures that would be expected if each broad category of benign explanation were correct. These signatures describe where the offsetting debits and credits must appear under U.S. GAAP.

Explanation Type	Expected Debit	Expected Credit	Where It Must Appear	Disclosure Implication
SSP / Breakage Change	Contract liability	Revenue (cumulative catch-up)	Income statement and contract balance rollforward	Disclosure of change in judgement under ASC 606

<b>Explanation Type</b>	<b>Expected Debit</b>	<b>Expected Credit</b>	<b>Where It Must Appear</b>	<b>Disclosure Implication</b>
Partner Prepayment	Cash	Deferred revenue / contract liability	Operating cash inflow; liability increase	Explanation of payment terms
Reinstatements / Make-goods	Expense or contra-revenue	Contract liability	Income statement line item identifiable	Disclosure of customer restitution
Revenue Reclassification	One revenue caption	Another revenue caption	Revenue footnote and comparatives	Explanation of presentation change
Extended Payment Terms	Noncurrent receivable	Current receivable	Balance sheet reclassification	MD&A liquidity discussion
Contract Asset Conditionality	Contract asset	Revenue	Contract asset disclosure	Explanation of conditionality
Collectibility Issue	Allowance for credit losses	Receivable	CECL allowance	Disclosure of credit risk
Acquisition Measurement Period	Goodwill	Acquired liability	Balance sheet and Note 2	ASC 805 measurement period disclosure
Platform Migration Revaluation	Revenue or goodwill	Contract liability	Income statement or goodwill	Explanation of remeasurement basis

Any benign explanation advanced by management must be consistent with one or more of the above signatures. Where the expected signature is absent from the published financial statements, the explanation is either incorrect or incomplete.

---

# 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%
<b>Total</b>	<b>265</b>	<b>100%</b>

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  $N = 265 \div r$ .

Assumed Reporting Rate (r)	Implied Victims (N)	Interpretation
5%	5,300	Very high reporting; implausible
2%	13,250	High reporting
<b>1%</b>	<b>26,500</b>	<b>Central estimate</b>
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:

- 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.
- 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.
- 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.
- 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
<b>Central victim estimate</b>	<b>26,500</b>	<b><math>265 \div 0.01</math></b>
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	$26,500 \times 217,831$
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.

# APPENDIX C: COMPARATIVE ANALYSIS METHODOLOGY

## C.1 Research Design and Objective

This analysis employs a systematic, multi-stage methodology to quantify and compare self-reported loyalty programme account compromises across five major U.S. airline Reddit communities. The research question asks: "Do self-reported account security incident rates differ significantly across airline loyalty program communities on Reddit?"

**Null Hypothesis ( $H_0$ ):** Incident rates do not differ significantly across airlines when normalized by community size.

**Alternative Hypothesis ( $H_1$ ):** At least one airline demonstrates a statistically significant difference in incident rate compared to others.

The study design is a comparative observational analysis of user-generated content from Reddit covering the period January 1, 2025 through December 5, 2025 (11 months).

## C.2 Data Collection Protocol

### Target Communities:

- r/AlaskaAirlines
- r/delta
- r/unitedairlines
- r/americanairlines
- r/SouthwestAirlines

**Search Parameters:** Two independent searches were conducted per airline: (1) posts containing 'hacked' in title OR body text, and (2) posts containing 'stolen' in title OR body text, with date filter applied for January 1, 2025 onwards.

**Data Fields Captured:** Post URL/permalink, post title, post body text (selftext), post creation date, post author username, comment text at all thread levels, comment author usernames, comment creation dates, and subreddit member counts (for normalization). The tool used to collect is [Instant Data Scraper Chrome Extension](#). The tool used to collect data within each post was the [Premium Octoparse Web Scraping Tool](#).

**Chain of Custody:** Collection date documented, data source recorded (third-party scraper tool name/version), raw data preserved in original format with no modifications to source text, subreddit member counts recorded with timestamp.

**Known Limitations:** Third-party scraper may not capture 100% of posts (official API preferred but access restricted). Reddit's search algorithm may not surface all historical posts. Deleted or removed posts not captured. Data represents snapshot at collection date, not real-time.

### C.3 Multi-Stage Filtering Framework

The methodology employs a three-stage filtering process to systematically reduce false positives while maintaining analytical rigor:

**Stage 2 - Automated Keyword Exclusion:** Five exclusion categories remove obvious false positives: (1) Travel tips/optimization content ("best hacks", "pro tips"), (2) Award program optimization ("loophole", "trick to get"), (3) Physical property theft ("luggage stolen", "bag stolen"), (4) Service complaints using metaphorical language ("stolen seat"), and (5) Tip-seeking questions ("what are the best hacks").

Implementation uses Google Sheets filter with case-insensitive exact phrase matching. Conservative approach: ambiguous cases pass through to next stage. Quality check: 10% random sample of excluded posts manually verified.

**Stage 3 - Lexicon-Based Triage Classification:** A rule-based binary text classifier using regular expressions (REGEX) and Boolean logic assigns each post to one of three priority categories:

*GROUP A (Attack/Compromise Semantic Field):*

REGEX pattern: (hack|hacked|hacking|hijack|stolen|stole|theft|fraud)

*GROUP B (Loyalty Programme Semantic Field):*

REGEX pattern: (mile|miles|points|lp|loyalty|mileage plan|frequent flier|frequent flyer|account)

*Classification Logic:*

- **HIGH:** Both Group A AND Group B match (probable loyalty account compromise)
- **MAYBE:** Group A matches but NOT Group B (possible security issue, incomplete evidence)
- **LOW:** Group A does not match (negligible probability of security incident)

This two-feature intersection classifier is transparent, deterministic, and reproducible.

**Stage 4 - Human Classification (HIGH-Priority Posts):** Systematic human review applies rigorous inclusion/exclusion criteria. All four inclusion criteria must be met: (1) Unauthorized account access claim, (2) Unauthorized redemption/transaction, (3) Temporal relevance (incident occurred in 2025), and (4) Genuine incident (not policy complaint).

For qualifying posts, all comments analyzed for additional victims using identical criteria. De-duplication protocol tracks usernames across entire dataset to prevent double-counting.

**Stage 5 - Human Classification (MAYBE-Priority Posts):** Brief scan to identify incidents misclassified due to missing loyalty program vocabulary. Most MAYBE posts are non-loyalty-account incidents; occasionally 1-2 posts per airline reclassified to HIGH.

## C.4 Incident Counting and De-Duplication

**Counting Protocol:** Total unique incidents = (Qualifying Posts + Qualifying Comments) - Duplicates

**De-Duplication Method:** Cross-referenced across: different posts, different search terms (hacked vs stolen), and post authors vs comment authors. If same username reports incident multiple times: count ONCE. If same username reports different incidents: count EACH separately.

## C.5 Normalisation and Statistical Analysis

**Normalization Methods:**

*Method 1 (Primary):* Incidents per 10,000 subreddit members  
 $\text{Rate}_1 = (\text{Unique Incidents} / \text{Subreddit Members}) \times 10,000$

Rationale: Adjusts for different community sizes; assumes community size correlates with customer base size.

*Method 2 (Secondary):* Incidents per 100 posts collected  
 $\text{Rate}_2 = (\text{Unique Incidents} / \text{Total Posts Collected}) \times 100$

Rationale: Controls for subreddit activity level and search result volume.

*Method 3 (Descriptive):* Raw incident count reported alongside normalized rates for full context.

## C.6 Quality Assurance and Bias Mitigation

**Consistency Verification:**

- Temporal consistency check: Compare classification decisions made early vs late in process
- Cross-airline consistency check: Ensure identical standards applied regardless of airline
- Edge case documentation maintained for all borderline classifications

### **Bias Mitigation Strategies:**

- Confirmation bias: Blind review where possible (reviewer doesn't know airline until after classification)
- Selection bias: Acknowledged that Reddit users are younger, more tech-savvy (affects all airlines equally)
- Reporting bias: Comparative design makes relative differences more meaningful than absolute rates
- Classification bias: Explicit criteria, multiple reviewers, inter-rater reliability testing
- Temporal bias: Date restriction to 2025 only
- Corporate response bias: Exclude 'thank you' posts that don't describe actual compromise

## **C.7 Limitations and Appropriate Use**

**Data Source Limitations:** Third-party scraper may not capture complete data. Reddit search algorithm limitations. Deleted/removed posts not captured. Point-in-time snapshot only.

**Sample Limitations:** Reddit users unrepresentative of general airline customers. Unknown reporting rate variation across airlines. Unknown proportion of total incidents captured. Subreddit size variation creates different base rates.

**Classification Limitations:** Human judgment subjectivity in ambiguous cases. Lexicon-based triage may miss non-standard vocabulary. Cannot independently verify authenticity of self-reports.

**External Validity Limitations:** Results specific to Reddit communities. May not reflect broader customer experience. Analysis identifies associations, not causal mechanisms.

**Honest Assessment:** This methodology provides best available evidence for comparative assessment given constraints (Reddit API access restrictions, resource limitations, time constraints) while maintaining scientific rigor and transparency. Results should be interpreted as indicative patterns in self-reported incidents on Reddit, not definitive counts of total security incidents.

Despite limitations, methodology remains valid for comparative purposes because: (1) same limitations apply to all airlines equally, (2) relative differences more robust than absolute rates, (3) transparent methods allow replication and verification, (4) multiple mitigation strategies implemented, and (5) conservative approach favors false negatives over false positives.

## C.8 Reproducibility and Transparency

**Documentation Requirements:** Complete documentation maintained for: collection date/timestamp, scraper tool name/version, search parameters, subreddit member counts, raw data files, Stage 2 exclusion terms and rates, exact REGEX formulas, classification spreadsheet with reasoning, de-duplication log, confidence levels, and statistical test results.

**Reproducibility Standard:** Another analyst could: collect same data using documented parameters, apply filters and reproduce exclusions, apply triage and reproduce classifications, read posts and reach similar conclusions, and replicate statistical calculations.

**Transparency Principles:** Complete disclosure of all methods. Honest acknowledgment of all limitations. No hidden steps or undocumented decisions. Raw data available for inspection (subject to privacy considerations). Reasoning for every classification decision documented. Alternative interpretations acknowledged. Uncertainty quantified where possible.

## C.9 Interpretation Guidelines

**Conservative Interpretation:** Results indicate patterns in self-reported incidents on Reddit. Not definitive counts of all security incidents. Comparative differences are more reliable than absolute rates. Statistical significance indicates a pattern unlikely due to chance alone.

### Appropriate Claims:

- "Analysis of Reddit posts suggests [Airline X] has higher self-reported incident rate"
- "Statistically significant difference detected ( $p < 0.05$ )"
- "Pattern consistent with [hypothesis]"

### Inappropriate Claims:

- "Proves [Airline X] has poor security"
- "Demonstrates [Airline X] is unsafe"
- "Shows exact number of security breaches"

**Required Context:** Results represent Reddit-reported incidents only. Multiple factors influence reporting behavior. Correlation does not imply causation. Findings should be considered alongside other evidence sources.

---

*Data Sources: Reddit subreddits r/AlaskaAirlines, r/delta, r/unitedairlines, r/americanairlines, r/SouthwestAirlines; collection period January 1 - November 30, 2025; third-party scraper tool (non-API access).*

---

# APPENDIX D: HACKS DATA COMPILATION METHODOLOGY

## D.1 Research Objective and Scope

The Hacks DataBook is a master dataset documenting 265 unique incidents of Alaska Airlines Mileage Plan account compromises reported publicly during calendar year 2025. The dataset was compiled through systematic search and verification protocols across multiple digital platforms to establish a baseline count of publicly documented account security incidents.

**Temporal Scope:** January 1, 2025 - November 30, 2025 (11 months)

**Research Question:** What is the minimum verifiable count of Alaska Airlines Mileage Plan account compromises reported publicly during 2025, and what patterns emerge from this documentation?

**Data Collection Method:** Manual search and cataloging of public posts, comments, articles, and reviews across multiple platforms, with dual-analyst verification of all entries.

## D.2 Search Protocol and Platform Coverage

### Search Terms and Variations:

Primary search queries focused on accounts of Alaska Airlines or Mileage Plan account compromises, including variations: "Alaska account hacked," "Mileage Plan stolen," "Alaska miles fraud," "Atmos account hacked" (post-merger terminology), and related combinations. Searches were conducted in English and, with translation, Chinese (US Card Forum).

### Platform Coverage:

Data collection indicated eight distinct platform categories:

1. **Reddit:** Multiple subreddits including r/AlaskaAirlines, /awardtravel
2. **FlyerTalk:** Alaska Airlines Mileage Plan forum threads and related discussions
3. **Facebook Groups:** Travel rewards communities (e.g., ROAM, Frequent Miler group), airline-specific groups, and credit card optimisation communities
4. **Twitter/X:** Public tweets mentioning Alaska Airlines and account security issues
5. **US Card Forum:** Chinese-language credit card rewards community ([www.uscardforum.com](http://www.uscardforum.com))
6. **LinkedIn:** Professional network posts discussing loyalty program security
7. **Review Platforms:** TrustPilot airline reviews mentioning account compromises
8. **News and Blogs:** Seattle Times articles, Frequent Miler blog posts, and other travel industry publications

## Search Execution:

Searches were conducted using platform-native search functions (Reddit search, Twitter search, Facebook group search, Google site-specific searches) as well as Google search with site operators (e.g., site:flyertalk.com "Alaska account hacked"). Search results were reviewed chronologically from January 2025 forward.

## D.3 Incident Identification and Initial Logging

When a potential incident was identified through search, it was immediately logged in the master DataBook (maintained as CSV file and Google Drive) with the following structured data fields:

### Field Structure:

Field Name	Format	Description	Preservation Standard
Ref	10XXX	Unique reference number for internal tracking	Sequential assignment
Date	DD-MMM-YY	Date of comment/post publication	As displayed on platform
Platform	Text	Source platform identifier	Standardized category
Username	Text	Original poster's username	Exact preservation
Miles Stolen	Numeric (with commas)	Quantity explicitly stated by victim	Verbatim formatting
Comment	Long text	Complete post/comment text	Verbatim transcription
Case ID	Case-XX	Thread grouping identifier	Sequential by thread
Comment Link	URL	Direct link to specific comment/post	Verified clickable
Thread Link	URL	Link to parent discussion thread	Verified clickable

Field Name	Format	Description	Preservation Standard
Evidence Link	URL	Supplementary evidence if applicable	Optional
Archive Link	URL	Permanent archive snapshot	archive.today or archive.ph
Notes	Text	Analyst observations or context	Optional
New?	Y/blank	Flag for recently added entries	Pending verification

### Data Entry Protocol:

All fields were populated at the time of initial discovery. The "Comment" field received particular attention, with complete verbatim transcription of the original post or comment text, including:

- Original spelling and grammar (apart from removal of commas for CSV compatibility)
- Punctuation and capitalization as written
- Informal language, abbreviations, emoticons
- No paraphrasing, summarization, or editorial modification

*Rationale:* Verbatim preservation maintains evidentiary integrity and allows independent analysts to assess tone, urgency, and credibility of victim reports without interpretive bias introduced by summarization.

## D.4 Verification and Quality Control Protocol

### Two-Analyst Verification Requirement:

Each potential incident underwent independent review by two separate data analysts to ensure inclusion criteria were met. This dual-verification process mitigated individual analyst bias and classification errors.

### Inclusion Criteria (ALL Five Must Be Met):

1. **Airline Specificity:** Incident must explicitly reference Alaska Airlines, Mileage Plan, or (post-September 2024) Atmos Rewards with clear context indicating Alaska's loyalty programme, or clearly implied based on forum and/or thread
2. **Account Compromise:** Clear indication that loyalty program account was accessed without authorisation (e.g., "my account was hacked," "someone got into my account," "unauthorised access")

3. **Fraudulent Redemption:** Miles/points were stolen, transferred, or used to book travel without account holder's permission (as opposed to mere phishing attempt without successful breach)
4. **Temporal Relevance:** Incident was reported during 2025 (post date within temporal scope)
5. **Verifiable Source:** Incident documented on accessible public platform with preserved link (not hearsay or private communication)

#### **Exclusion Criteria (ANY One Disqualifies):**

1. **Non-Alaska Incidents:** Loyalty program breaches at United, Delta, American, Southwest, or other carriers
2. **Security Concerns Without Actual Incident:** Posts expressing worry about potential vulnerabilities without confirming an actual compromise occurred
3. **Service Complaints Without Compromise:** General Alaska service quality complaints, devaluation protests, or policy disagreements not involving account security
4. **Duplicate Reports:** Same username reporting identical incident across multiple platforms (counted once)

## **D.5 Data Preservation and Chain of Custody**

### **Archive Protocol:**

All incidents were archived using third-party archiving services to create permanent, timestamped snapshots of original content. Two archiving services were employed:

- **archive.today** (Primary): Provides immediate snapshot and permanent URL
- **Hunchly** (Secondary): Backup service for websites unable to be archived

*Rationale:* Archiving ensures evidence preservation in case original content is deleted, platforms change access policies, or accounts are suspended. Permanent archives provide timestamped proof of content existence and enable independent verification by third parties.

### **Chain of Custody Documentation:**

For each incident, the following custody trail was maintained:

- **Discovery:** Date incident first identified by analyst
- **Verification:** Date second analyst completed review
- **Archive:** Timestamp of archive.today snapshot

## D.6 Case Grouping Methodology

### Case Definition:

A "Case" represents a single discussion thread, article, or social media post and all associated comments within that thread. Case grouping enables:

- De-duplication of multiple victims reporting in same thread
- Preservation of discussion context
- Analysis of community response patterns
- Tracking of how information spreads across thread

### Case ID Assignment:

Case IDs (format: Case-01, Case-02, etc.) were assigned chronologically based on when the parent thread or article was first identified during the search process. The dataset contains 73 unique Cases, with multiple victim reports often appearing within popular or high-visibility threads.

### Single-Thread Grouping:

All comments within one Reddit thread, FlyerTalk discussion, or Facebook post received the same Case ID. For example:

- Case-20: Reddit thread "Just noticed I had 250,000 miles fraudulently redeemed" contains 23 victim reports across post author and commenters
- Case-32: Facebook group post contains 14 victim reports from different users
- Case-72: Seattle Times article contains 8 victim reports in comment section

## D.7 De-Duplication Protocol

### Username Tracking:

All usernames were tracked across the entire dataset to identify potential duplicate reports.

### De-Duplication Rules:

1. **Same Username, Same Incident, Multiple Comments:** If username reports same incident multiple times within one thread, count once (earliest mention preserved, with other comments added to same text box)
2. **Same Username, Same Incident, Multiple Platforms:** If username reports same incident on Reddit and Twitter, count once (both preserved in DataBook)
3. **Same Username, Different Incidents:** If username reports distinct incidents at different times (e.g., hacked in January, hacked again in July), count separately

4. **Different Usernames, Suspicious Similarity:** Flagged for review but generally counted separately unless definitive proof of same individual

#### Unique Incident Determination:

Final unique incident count = Total logged incidents - Identified duplicates

## D.8 Quantitative Data Extraction

#### Miles Stolen Field Methodology:

When victims explicitly stated the quantity of miles stolen, this figure was captured exactly as written in the original post. No standardization, estimation, or inference was applied.

#### Capture Rules:

- **Explicit Statement Required:** Miles quantity included only if victim stated specific number (e.g., "250,000 miles stolen")
- **Format Preservation:** Original number formatting preserved including commas, spaces, or other separators
- **No Estimation:** If victim wrote "most of my miles" or "a lot of points," Miles Stolen field left blank
- **No Conversion:** If victim stated dollar value instead of miles, not converted (left blank)
- **Range Handling:** If victim stated "200,000-300,000 miles," midpoint not calculated (preserved as written or left blank)

#### Quantification Statistics:

Of 265 total incidents documented:

Category	Count	Percentage	Notes
Miles Explicitly Quantified	80	30.2%	Victim stated specific number
Miles Not Quantified	185	69.8%	Victim described theft without quantity
<b>Total Incidents</b>	<b>265</b>	<b>100%</b>	Complete dataset

### Quantified Theft Distribution:

Among the 80 incidents with explicit mile quantification:

Statistic	Value	Derivation
Minimum theft	25,000 miles	Lowest quantified incident
Maximum theft	800,000 miles	Highest quantified incident
<b>Mean theft</b>	<b>217,831 miles</b>	Sum of 80 quantified thefts ÷ 80
Median theft	150,000 miles	50th percentile of sorted distribution
75th percentile	255,000 miles	Third quartile
90th percentile	350,000 miles	Ninth decile

*Rationale:* The 30.2% quantification rate likely introduces selection bias, as victims suffering larger losses may be more motivated to state specific amounts. The mean of 217,831 miles should therefore be interpreted as potentially representing higher-value incidents rather than a representative average across all 265 cases.

## APPENDIX E: UNDERSTANDING THE MILEAGE PLAN: AN ACCOUNTING PRIMER

Before examining the anomalies, some readers may benefit from understanding how loyalty programme transactions flow through Alaska's financial statements. This context may prove insightful in appreciating why the Q2 2025 deviation is so significant.

Alaska operates the Mileage Plan through a co-branded credit card partnership with Bank of America.

Under ASC 606, Alaska allocates the cash it receives from Bank of America between two components: a **marketing and brand component**, recognised immediately as "loyalty programme other revenue"; and a **transportation component**, recorded as a deferred revenue liability until miles are redeemed or expire (breakage).

Based on Alaska's disclosures, the loyalty programme economics appear to be presented on a relatively **net** basis (with certain partner costs offset within "loyalty programme other revenue"), whereas some peer airlines report comparable items on a more **gross** basis. This difference in presentation practice can materially affect cross-carrier comparisons of loyalty revenue and margins.

In simplified terms, the economic flow is as follows. First, Bank of America purchases miles: as cardholders earn miles on spend, Bank of America buys those miles from Alaska at a contracted price per mile. The exact rate is not disclosed. Based on the relationship between reported loyalty revenue and liability movements, the all-in price could be in the region of **c. 1.25 cents per mile**, purely as an analytical estimate.

Second, Alaska records a portion as a liability: a portion of that price per mile is allocated to the future transportation obligation and recorded as an increase in the loyalty deferred revenue balance ("increase in liability for loyalty points issued"). From the 2024 10-K data, this implied standalone selling price (SSP) is estimated at roughly **c. 0.75 cents per mile**. This number is not disclosed directly; it is inferred from the relationship between miles issued and the associated liability.

Third, Alaska records the remainder as revenue: the residual portion of the price per mile (the difference between the total price and the SSP transportation component) is recognised immediately as "loyalty programme other revenue", reflecting the brand, marketing and access-to-customer-list value that Alaska provides to Bank of America.

Fourth, Alaska recognises deferred revenue as miles are redeemed: when miles are redeemed, Alaska releases the relevant portion of deferred revenue. Redemptions on Alaska's own metal

appear as "loyalty redemptions - passenger revenue". Redemptions on partner airlines reduce the loyalty liability and give rise to a reimbursement expense to partners; the net margin between the SSP value released and the partner reimbursement cost effectively flows through "loyalty programme other revenue".

There are two further flows that influence the key metrics in this report. Miles are also awarded on flown tickets. These miles increase the loyalty deferred revenue ("liability for points issued") but are funded out of ticket revenue rather than Bank of America consideration. They therefore increase the numerator of the issuance-to-revenue ratio without directly increasing "loyalty programme other revenue". Additionally, for partner redemptions, Alaska reimburses partners at a contractual rate per mile. If that reimbursement rate is below the SSP, the programme generates a positive margin on those redemptions. If the reimbursement rate is above the SSP, the margin is negative.

Despite these additional moving parts, the **issuance-to-revenue ratio** provides a useful analytical proxy for the underlying economics of the loyalty programme: it captures how many dollars of new loyalty liability ("miles issued") are being created for each dollar of "loyalty programme other revenue" recognised in the same quarter. As shown below, this ratio has historically been remarkably stable.

# APPENDIX F: FINANCIAL EXPOSURE METHODOLOGY

## F.1 Overview and Purpose

This appendix documents the methodology underlying the financial exposure estimates presented in the Executive Summary. The analysis quantifies potential losses across four categories: direct fraud losses, restatement/impairment risk, regulatory penalties, and litigation reserves.

**Key Finding:** The calculated exposure range of **\$114M to \$692M** (29% to 175% of 2024 net income) demonstrates material financial risk regardless of scenario assumptions. The central estimate of **\$301M** represents 76% of Alaska's 2024 net income of \$395M.

## F.2 Direct Fraud Losses

### Methodology

Direct fraud losses represent the economic cost Alaska incurs when it reimburses partner airlines for fraudulently redeemed miles, then restores those miles to victim accounts.

**Calculation:** Estimated Victims × Average Miles Stolen × Standalone Selling Price

### Inputs

Parameter	Conservative	Central	Aggressive	Basis
Estimated Victims	13,250	26,500	53,000	Appendix B: 0.5x to 2x central
Miles per Victim	217,831	217,831	217,831	80 quantified incidents
SSP per Mile	\$0.0075	\$0.0075	\$0.0075	Inferred from 2024 10-K

## Results

Scenario	Total Miles Stolen	Direct Loss
Conservative	2.89 billion	<b>\$21.6M</b>
Central	5.77 billion	<b>\$43.3M</b>
Aggressive	11.54 billion	<b>\$86.6M</b>

## Validation

The central estimate of \$43.3M aligns with the independently calculated excess partner redemptions of \$45M from Schedule 4 (95% convergence), providing corroboration through two independent methodologies.

---

## F.3 Potential Restatement / Impairment

### Methodology

This category captures the risk that assets currently on Alaska's balance sheet may require write-down or restatement upon audit scrutiny.

### Identified Anomalies:

- Q2-Q3 2025 "Other Non-Current Assets" increase: \$120M (no explanatory disclosure)
- Q4 2024 retroactive restatement of affinity receivables: \$58M (characterised as "immaterial")

### Calculation

Parameter	Conservative	Central	Aggressive	Basis
Identified Anomaly	\$120M	\$178M	\$178M	NCA increase alone vs. with restatement
Impairment Probability	50%	75%	100%	Likelihood of required write-down
<b>Expected Value</b>	<b>\$60.0M</b>	<b>\$133.5M</b>	<b>\$178.0M</b>	Anomaly × Probability

## Rationale for Probability Estimates

**Conservative (50%):** Assumes benign explanation exists but was not disclosed; 50% probability management cannot adequately explain the movements to auditors.

**Central (75%):** Reflects the difficulty of explaining a  $10.40\sigma$  statistical anomaly combined with undisclosed balance sheet reclassification. The "GAAP trap" analysis (Appendix A.8) found all ten benign hypotheses failed on quantitative, temporal, or disclosure grounds.

**Aggressive (100%):** Assumes the full identified amount requires recognition as expense or impairment.

---

## F.4 Regulatory Penalties

### Methodology

Regulatory exposure is estimated by identifying potential violations, matching them to applicable statutes, and calibrating penalty ranges against recent enforcement precedents.

#### F.4.1 SEC - Financial Reporting Violations

##### Potential Violations:

1. Material misstatement under SAB 99 (\$58M = 15% of NI; \$120M = 30% of NI)
2. Cybersecurity disclosure failure (Form 8-K rules effective December 2023)
3. Internal controls deficiency under SOX 404

### Precedent Analysis:

Case	Year	Penalty	Violation Type
Fluor Corporation	2023	\$14.5M	Accounting errors materially overstated earnings
Newell Brands	2023	\$12.5M	Misleading investors on core sales growth
Unisys (SolarWinds)	2024	\$4.0M	Cyber disclosure + controls deficiency
Blackbaud (SEC)	2024	\$3.0M	Misleading cybersecurity disclosures
Avaya/Check Point/Mimecast	2024	\$1M each	Downplaying cyber incident severity

### Key Precedent Notes:

The SolarWinds-related enforcement actions (October 2024) are particularly instructive. The SEC penalised four companies that were *victims* of the SolarWinds cyberattack for misleading disclosures about its impact:

- Unisys described risks as "hypothetical" despite gigabytes of data exfiltration
- Avaya stated "limited" email access but omitted 145 files in cloud environment
- All four companies settled for \$1M-\$4M

The SEC's position: "Federal securities laws prohibit half-truths, and there is no exception for statements in risk-factor disclosures."

**Estimate Range:** \$4M (SolarWinds-type) to \$25M (Fluor-type with cyber overlay)

**Central Estimate:** \$12.5M

### F.4.2 DOT - Consumer Protection & Merger Condition Violations

#### Potential Violations:

1. Breach of merger conditions (CEO personally signed September 2024 agreement)
2. Unfair/deceptive practices under 49 USC §41712
3. Terms change imposing new limits contrary to merger commitments

## Merger Agreement Analysis:

The DOT-mandated merger agreement (September 2024) included binding commitments:

*"[Alaska shall not] decrease the dollar value, eliminate, reduce, suspend, forfeit, invalidate, impose new limits on access, use, redemption, or validity, or impose new requirements..."*

Alaska's subsequent actions that potentially conflict:

- Telephone-only booking restriction imposed on hack victims
- Terms amendment adding: "regardless of member fault" revocation authority
- "System or partner issues" clause permitting point clawback

## Precedent Analysis:

Case	Year	Penalty	Violation Type
Southwest Airlines	2023	\$140M	Consumer protection - operational failure
American Airlines	2024	\$50M	Wheelchair/disability service failures
Maximum per violation	2025	\$75,000	Per 49 USC §41712 (inflation-adjusted)

## Per-Violation Calculation:

If DOT determines each victim (26,500 central estimate) suffered an unfair practice violation:

- Per-violation penalty: \$75,000
- Theoretical maximum: \$1.99 billion

In practice, settlements are substantially lower. The Southwest \$140M penalty involved ~16,900 passengers with delayed refunds.

**Estimate Range:** \$5M (negotiated settlement) to \$50M (aggressive enforcement)

**Central Estimate:** \$20M

**Note on Regulatory Scrutiny:** The DOT publicly stated it is "closely reviewing all changes to Alaska's rewards program to assess compliance with the terms under the merger agreement" (October 2024).

#### F.4.3 Washington State Attorney General

**Applicable Law:** RCW 19.255.010 requires notification to WA AG within 30 days of discovering a breach affecting more than 500 Washington residents.

**Violation Assessment:**

- Alaska headquarters: Seattle, Washington
- Estimated WA victims: ~1,325 (5% of 26,500)
- Public breach notifications filed: None identified

**Precedent: Blackbaud Multistate Settlement (October 2023)**

The Blackbaud settlement provides a direct precedent for data breach notification failures:

Metric	Value
Total settlement	\$49.5M
States participating	50 + DC
Lead states	Indiana, Vermont
Washington allocation	~\$2.9M
New York allocation	\$2.9M
Victims affected	13,000+ organisations

Key finding: Blackbaud "failed to provide its customers with timely, complete, or accurate information regarding the breach, as required by law."

**Estimate Range:** \$1M to \$10M

**Central Estimate:** \$3M

#### F.4.4 FTC - Unfair/Deceptive Practices

**Potential Violations:**

- Section 5 FTC Act: failure to implement reasonable data security
- Deceptive representations regarding account security

### Precedent Analysis:

Case	Year	Penalty	Violation Type
Avast	2024	\$16.5M	Sold browsing data despite privacy claims
Verkada	2024	\$2.95M	Data security failures + CAN-SPAM
InMarket Media	2024	Consent order	Location data without consent
X-Mode Social	2024	Consent order	Sensitive location data sales

### FTC Enforcement Philosophy (2024):

Chair Lina Khan has emphasised enforcement against companies with security failures leading to sensitive data exposure. The FTC views loyalty programme data (travel patterns, spending habits) as sensitive information warranting heightened protection.

**Estimate Range:** \$3M to \$15M

**Central Estimate:** \$10M

### F.4.5 CFPB - Credit Card Rewards Programme Violations

#### Regulatory Framework:

The Consumer Financial Protection Bureau has explicitly targeted airline loyalty programmes as an enforcement priority:

#### CFPB Circular 2024-07 (December 2024):

"When credit card issuers promise cashback bonuses or free round-trip airfares, they should actually deliver them. The CFPB is taking aim at bait-and-switch tactics."

The Circular identifies potentially illegal practices including:

- Devaluing earned rewards without adequate notice
- Hiding conditions for earning or keeping rewards in fine print

- Failing to deliver promised benefits due to technical or operational failures
- Sudden forfeiture of earned rewards

### **May 2024 Joint CFPB-DOT Hearing:**

Director Chopra and Secretary Buttigieg jointly examined airline rewards programmes. Chopra compared rewards points to "savings accounts" and announced four enforcement priorities:

1. Protect points from devaluation
2. Stop bait-and-switch schemes
3. Ensure redemption is possible
4. Promote fair competition

### **Application to Alaska:**

Alaska's practices potentially implicate multiple CFPB concerns:

1. **Account Restrictions:** Telephone-only booking requirement materially degrades redemption utility for hack victims
2. **One-Time Courtesy Framing:** May constitute deceptive practice if security failure was systemic
3. **Terms Amendment:** "Regardless of member fault" revocation authority may violate UDAAP

### **CFPB Enforcement Authority:**

- Section 5 UDAAP violations: Up to \$50,120 per violation (2024)
- Restitution authority: Full consumer harm recovery
- Referral to State AGs: CFPB can coordinate multistate enforcement

**Estimate Range:** \$5M to \$25M

**Central Estimate:** \$12M

F.4.6 Other Agencies Considered

Agencies Not Quantified:

Agency	Potential Concern	Reason Excluded
DOJ/FBI	Organised fraud ring investigation	No direct penalty to Alaska
CBP	Fraudulent passengers entering US	No airline penalty mechanism
GDPR	EU citizen victims	Speculative; no evidence
State AG Coalition	Multistate action	Captured in Litigation (F.5.5)

F.4.7 Regulatory Penalty Summary

Agency	Conservative	Central	Aggressive	Key Precedent
SEC	\$4M	\$12.5M	\$25M	Unisys/Fluor
DOT	\$5M	\$20M	\$50M	Southwest/merger
WA AG	\$1M	\$3M	\$10M	Blackbaud
FTC	\$3M	\$10M	\$15M	Avast
CFPB	\$5M	\$12M	\$25M	Circular 2024-07
Total	\$18M	\$57.5M	\$125M	

---

## F.5 Litigation Reserves

### F.5.1 Securities Class Action

#### F.5.1.1 Industry Statistics

**Basis:** Cornerstone Research annual reports on securities class action filings and settlements (2023-2024).

Metric	2024 Value	2023 Value	Source
Median SCA settlement	\$14M	\$15M	Cornerstone 2024
Average SCA settlement	\$42.4M	\$48.7M	Cornerstone 2024
Accounting case average	\$30.1M	\$47M	Cornerstone 2024
Mega settlements (>\$100M)	7	9	Cornerstone 2024
Filing probability (S&P 500)	6.1%	7.1%	Cornerstone 2024

#### F.5.1.2 Boeing Company Precedent

The Boeing securities litigation provides a directly analogous precedent for Alaska. Boeing faced securities claims arising from safety failures and disclosure deficiencies:

##### **SEC Fair Fund (September 2022):**

- Penalty: \$200M (subsequently rounded to \$201M with interest)
- Violation: Materially misleading statements following 737 MAX crashes
- Key finding: Boeing's internal Safety Review Board had concluded MCAS was "an airplane safety issue" requiring remediation, but this was not disclosed
- Relevance: Demonstrates SEC willingness to impose substantial penalties for disclosure failures concerning known internal problems

##### **Private Securities Class Action (ongoing):**

- Class period: November 2018 to December 2019 (first action); October 2019 to January 2024 (second action)
- Lead plaintiff: Employees' Retirement System of Rhode Island
- Status: Class certified March 2025; discovery ongoing

- Allegations: False statements regarding safety systems and manufacturing quality
- Projected settlement range: \$100M-\$300M based on comparable cases

#### **Boeing Derivative Settlement (March 2022):**

- Settlement: \$237.5M (second-largest insurer-funded derivative settlement in history)
- Governance reforms: separation of CEO/Chair roles; enhanced safety oversight reporting
- Relevance: Demonstrates substantial exposure for board-level oversight failures

#### **F.5.1.3 ALK-Specific Filing Probability Assessment**

Filing probability is elevated significantly above baseline due to:

1. **10.40 $\sigma$  Statistical Anomaly:** An event of this magnitude has a probability of approximately 1 in 10<sup>24</sup> under normal distributional assumptions. This is unprecedented among airline peers and provides clear grounds for allegations of undisclosed material information.
2. **Undisclosed Balance Sheet Reclassification:** The \$120M movement to "Other Non-Current Assets" without explanatory disclosure raises questions about potential asset impairment and earnings management.
3. **Retroactive Restatement:** The \$58M (49%) restatement of Q4 2024 affinity receivables, characterised as "immaterial" despite representing 15% of net income, provides a documented pattern of questionable materiality judgements.
4. **Cybersecurity Incident Non-Disclosure:** If the Hawaiian Airlines breach (disclosed June 2025) facilitated Mileage Plan compromises, failure to disclose material cybersecurity impacts would trigger SEC cybersecurity disclosure rules effective December 2023.
5. **SOX 404 Internal Control Implications:** The pattern of anomalies suggests potential material weaknesses in internal controls over financial reporting, particularly regarding loyalty programme accounting.

**Filing Probability Estimate:**

Scenario	Probability	Rationale
Conservative	40%	Statistical anomaly alone sufficient for filing
Central	60%	Anomaly + non-disclosure pattern
Aggressive	80%	Full pattern including restatement + cybersecurity

F.5.1.4 Settlement Range Assessment

Settlement Tier	Amount	Comparable Cases
Median accounting case	\$12M-\$14M	Cornerstone 2024 data
Average accounting case	\$30M	Cornerstone 2024 data
Boeing-type disclosure failure	\$50M-\$100M	Boeing Fair Fund, Fluor
Mega settlement (material fraud)	\$150M-\$250M	Boeing derivative, Wells Fargo

**ALK Settlement Range by Scenario:**

Parameter	Conservative	Central	Aggressive
Filing Probability	40%	60%	80%
Settlement if Filed	\$20M	\$50M	\$150M
Expected Value	\$8.0M	\$30.0M	\$120.0M

---

F.5.2 Consumer Class Action - Mileage Plan Account Holders

F.5.2.1 Legal Framework and ADA Preemption Considerations

The Airline Deregulation Act (ADA) of 1978 broadly preempts state law claims "related to a price, route, or service of an air carrier." This creates significant but not insurmountable barriers for consumer class actions against airlines.

## Key Precedents:

*Northwest, Inc. v. Ginsberg* (U.S. Supreme Court, 2014):

- Held that implied covenant of good faith claims are preempted when based on state-imposed obligations
- However, the Court explicitly preserved breach of contract claims based on voluntary contractual undertakings
- The Court noted that "had Ginsberg pursued his contract claim, he might have been able to prove that Northwest did not have unfettered discretion to terminate his membership"

*American Airlines v. Wolens* (U.S. Supreme Court, 1995):

- Permitted breach of contract claims relating to frequent flyer programme restrictions
- Distinguished between enforcing contractual terms (permitted) and expanding obligations through state law (preempted)

## Application to Alaska:

Alaska's terms amendment adding "regardless of member fault" revocation authority may create viable contract claims:

1. **Breach of Contract:** If prior terms promised security and account protection, unilateral amendment may breach implied contractual undertakings
2. **Data Breach Claims:** The ADA does not preempt claims unrelated to rates, routes, or services. Data security failures may fall outside preemption scope
3. **CFPB Enforcement:** Federal consumer protection laws (UDAAP) are not preempted by the ADA

## CrowdStrike Litigation Distinction:

The June 2025 dismissal of class action claims against CrowdStrike (re: airline passengers affected by the July 2024 outage) confirms broad ADA preemption but is distinguishable:

- CrowdStrike claims were pure flight disruption claims
- Alaska claims would focus on data security failures and account restrictions, which may be collateral to airline services

### F.5.2.2 Existing Alaska Airlines Class Action

A class action has already been filed against Alaska Airlines regarding the Flight Pass programme:

### **Burton v. Alaska Airlines (August 2025):**

- Allegation: Alaska reduced Flight Pass benefits by 50% while maintaining subscription prices
- Class definition: Nationwide subscribers affected by September 2024 changes
- Status: Pending

This establishes plaintiffs' counsel familiarity with Alaska and creates a template for Mileage Plan-specific claims.

#### F.5.2.3 American Airlines Loyalty Account Precedent

### **Nachison v. American Airlines (California, January 2024):**

- Allegation: Wrongful termination of AAdvantage accounts; loss of 550,000+ miles each
- Class definition: AAdvantage members whose accounts were terminated
- Status: Ongoing
- Relevance: Demonstrates class certification viability for loyalty programme disputes

#### F.5.2.4 Data Breach Settlement Precedents

Recent data breach class action settlements provide benchmarks for per-victim recovery:

Case	Settlement	Victims	Per-Victim	Year
Equifax	\$425M	147M	\$2.89	2019
AT&T	TBD	TBD	Up to \$2,500 documented	2025
Cencora	\$40M	TBD	Up to \$5,000 documented	2025
Prudential	\$4.75M	TBD	\$200-\$599 per SSN	2025
Frontier	\$5.6M	750K	Up to \$5,000 documented	2025
Panera	\$2.5M	147K	Up to \$6,500 documented	2025

### **Typical Structure:**

- Flat payment option: \$25-\$150 (no documentation required)
- Documented losses: Up to \$2,500-\$10,000 (with receipts)
- Extraordinary losses: Up to \$35,000 in some cases

#### F.5.2.5 Consumer Class Action Calculation

##### Potential Claims:

1. **Account Restriction Class:** High-value members forced into telephone-only booking
2. **Data Breach Class:** Members whose personal information was accessed
3. **Terms Violation Class:** Members adversely affected by unilateral terms changes

##### Calculation:

Parameter	Conservative	Central	Aggressive
Potential Class Size	13,250	26,500	53,000
Likelihood of Filing	50%	70%	85%
Per-Member Recovery	\$150	\$500	\$1,500
<b>Expected Value</b>	<b>\$1.0M</b>	<b>\$9.3M</b>	<b>\$67.6M</b>

**Note:** ADA preemption creates significant uncertainty. The central estimate assumes partial success on data breach claims while rates/routes/services claims are dismissed.

---

#### F.5.3 Shareholder Derivative Action

##### F.5.3.1 Boeing Derivative Precedent

The Boeing derivative settlement (\$237.5M, March 2022) demonstrates substantial board-level exposure for oversight failures. Key features:

- Largest-ever Delaware Chancery Court derivative settlement
- Required governance reforms: CEO/Chair separation, safety oversight enhancements
- Board members did not admit liability but faced significant reputational consequences

##### F.5.3.2 ALK Derivative Exposure

Potential claims against Alaska's board:

1. **Failure to Monitor Cybersecurity:** Board oversight of IT security and data protection
2. **Failure to Disclose:** Oversight of SEC reporting and disclosure controls
3. **Breach of Merger Commitments:** Board responsibility for DOT compliance

### Calculation:

Parameter	Conservative	Central	Aggressive
Filing Probability	25%	40%	60%
Settlement if Filed	\$10M	\$25M	\$75M
<b>Expected Value</b>	<b>\$2.5M</b>	<b>\$10.0M</b>	<b>\$45.0M</b>

---

## F.5.4 CFPB Enforcement and Private Right of Action

### F.5.4.1 CFPB Regulatory Focus on Loyalty Programmes

The CFPB has explicitly targeted airline loyalty programmes as an enforcement priority:

#### **CFPB Circular 2024-07 (December 2024):**

- Issued to all law enforcement agencies
- Warns that credit card rewards devaluation may constitute UDAAP violations
- Specifically addresses "hiding conditions for earning or keeping rewards"
- Notes that "sudden forfeiture of earned rewards upon account closure" is problematic

#### **May 2024 Joint CFPB-DOT Hearing:**

- Director Chopra compared rewards points to "savings accounts"
- Identified four enforcement priorities: (1) protect points from devaluation; (2) stop bait-and-switch; (3) ensure redemption; (4) promote competition

### F.5.4.2 Alaska-Specific CFPB Exposure

Alaska's practices potentially implicate CFPB guidance:

1. **Account Restrictions:** Telephone-only booking requirement degrades redemption utility
2. **One-Time Courtesy Framing:** May constitute deceptive practice if security failure was systemic
3. **Terms Amendment:** "Regardless of member fault" clause may be unfair practice

### Calculation:

CFPB-referred private actions or state AG enforcement actions typically yield:

Parameter	Conservative	Central	Aggressive
Likelihood of CFPB Referral	20%	35%	50%
Settlement if Referred	\$5M	\$15M	\$40M
<b>Expected Value</b>	<b>\$1.0M</b>	<b>\$5.3M</b>	<b>\$20.0M</b>

---

## F.5.5 Multistate Attorney General Action

### F.5.5.1 DOT-State AG Partnership (April 2024)

In April 2024, DOT announced the "Airline Passenger Protection Partnership" with 18 states and territories, empowering state AGs to investigate airline consumer complaints and refer cases to DOT for enforcement.

**Participating States Include:** California, Colorado, Connecticut, Illinois, Maine, Maryland, Michigan, Nevada, New York, New Hampshire, North Carolina, Oklahoma, Pennsylvania, Rhode Island, Wisconsin, and others.

**Washington State (Alaska's headquarters) is notably positioned** to investigate Mileage Plan complaints under this partnership framework.

### F.5.5.2 Multistate Enforcement Precedent

Case	States	Settlement	Year	Violation Type
Blackbaud	50 + DC	\$49.5M	2023	Data breach notification
Equifax	50 + DC	\$175M (to states)	2019	Data breach + consumer harm
T-Mobile	50 + DC	\$350M	2022	Data breach
Uber	50 + DC	\$148M	2018	Data breach notification delay

**Calculation:**

Parameter	Conservative	Central	Aggressive
Likelihood of Multistate Action	15%	30%	50%
Settlement if Filed	\$15M	\$40M	\$100M
<b>Expected Value</b>	<b>\$2.3M</b>	<b>\$12.0M</b>	<b>\$50.0M</b>

---

## F.5.6 Litigation Reserve Summary

Category	Conservative	Central	Aggressive
Securities Class Action	\$8.0M	\$30.0M	\$120.0M
Consumer Class Action	\$1.0M	\$9.3M	\$67.6M
Shareholder Derivative	\$2.5M	\$10.0M	\$45.0M
CFPB-Related Actions	\$1.0M	\$5.3M	\$20.0M
Multistate AG Action	\$2.3M	\$12.0M	\$50.0M
<b>TOTAL LITIGATION</b>	<b>\$14.8M</b>	<b>\$66.6M</b>	<b>\$302.6M</b>

The litigation reserve reflects:

1. Boeing-calibrated securities exposure (Fair Fund + class action precedents)
  2. Existing Alaska Airlines Flight Pass class action (demonstrates plaintiffs' bar interest)
  3. CFPB's explicit targeting of airline loyalty programmes
  4. DOT-State AG partnership enabling coordinated enforcement
  5. Multistate data breach enforcement trend
  6. Shareholder derivative action exposure (Boeing \$237.5M precedent)
-

## F.6 Grand Summary

### Calculated Financial Exposure

Category	Conservative	Central	Aggressive
Direct Fraud Losses	\$21.6M	\$43.3M	\$86.6M
Restatement/Impairment	\$60.0M	\$133.5M	\$178.0M
Regulatory Penalties	\$18.0M	\$57.5M	\$125.0M
Litigation Reserves	\$14.7M	\$66.5M	\$302.6M
<b>TOTAL</b>	<b>\$114.3M</b>	<b>\$300.8M</b>	<b>\$692.2M</b>

### Materiality Context

Metric	Conservative	Central	Aggressive
As % of 2024 Net Income	29.0%	76.2%	175.2%
As % of 2024 Total Revenue	1.1%	3.0%	6.9%
As % of 2024 Total Assets	0.5%	1.5%	3.3%

---

## F.7 Limitations and Caveats

- Precedent Applicability:** Past enforcement actions and settlements may not predict future outcomes, particularly for unprecedented violation types (e.g., merger condition breach).
- Cooperation Credit:** Estimates do not assume cooperation credit. If Alaska self-reports and cooperates, penalties could be 50-70% lower based on SEC statistics.
- Political Environment:** Regulatory enforcement priorities shift with administrations. The estimates assume continuation of 2023-2024 enforcement postures.
- Management Explanation:** If Alaska provides adequate explanations for the accounting anomalies, restatement/impairment risk could be substantially lower.

5. **Discovery:** Actual litigation outcomes depend on discovery processes that may reveal facts not apparent from public filings.

---

*Data Sources: SEC EDGAR filings (ALK 2022-2025), Cornerstone Research (Securities Class Action Settlements 2024, Accounting Class Action 2024), SEC Press Releases (October 2024 SolarWinds enforcement, September 2022 Boeing Fair Fund), DOT Press Releases (Southwest 2023, American 2024, April 2024 State AG Partnership), NY AG Press Release (Blackbaud 2023), FTC Press Releases (2024 enforcement actions), CFPB Circular 2024-07 (December 2024), RCW 19.255.010, 49 USC §41712, Northwest Inc. v. Ginsberg (U.S. Supreme Court 2014), American Airlines v. Wolens (U.S. Supreme Court 1995), Boeing derivative settlement (Delaware Chancery Court, March 2022), Top Class Actions (Burton v. Alaska Airlines, August 2025; Nachison v. American Airlines, January 2024).*

---

Ref #	Date	Platform	Username	Miles Stolen	Comment
#10001	03-Jan-25	FlyerTalk	PaceLaw2012	255,000	HELP: Someone hacked my AS account - 255K miles gone! Is AS under attack? Just checked my AS balance to see if my first flight of the year posted and I saw that someone booked a QR flight from PVG to JFK for 255k miles for someone. Activity page says Qatar Airways QR PVG-JFK DPVFER Yioing Wang Redeemed -255000. I am not Yioing Wang. I never received a confirmation email or otherwise would have stopped it immediately. I was also the subject of a spam bomb attack on my primary email 2 weeks ago but I managed to change all my email addresses. I also see this message when I go to my account main page: Mileage Program Discrepancies The Mileage Program account has some discrepancies. Contact Customer Care for assistance at 1-800-654-5669 Monday-Friday 7:00 a.m. - 7:00 p.m. (PT) and Saturday 8:00 a.m. - 5:00 p.m. (PT) Anyone else getting this? Currently on the phone with customer service. Hoping to get a resolution soon!
#10002	06-Jan-25	Reddit	ComplaintKooky7504	80,000	80000+ points transferred out of my Alaska account I just noticed that almost all my Alaska points were transferred out of my account the week of Christmas and it was not me. My primary contact email and phone number was changed on my account too and I never got a email or notification from Alaska that my primary contact information was changed. I am waiting for Alaskas customer support phone number to open and given them a call to figure out what the hell has happened. Obviously I got hacked but I am very surprised I received no notification or anything from Alaska when my primary contact information was changed. Has anyone ever experienced this?
#10003	06-Jan-25	Reddit	landonfox	800,000	They've been telling me its coming soon for years now. Pretty pathetic most local credit unions have it figured out but they can't. I also had my miles stolen over 800k of them actually. They reimbursed me but told me that was a one time thing and that I should put a pin in. Problem is I buy flights weekly and sometimes there is a 45+ minute wait on hold. And its not their 24/7 reservation team that can do it its the tech team that closes at night so lots a times I was stuck unable to buy flights at all when I wanted to. Ultimately I removed my pin and am just crossing my fingers until they can get MFA/2FA. Sure with the merger it will be even longer
#10004	06-Jan-25	Reddit	Past_Commission_3733		This happened to me a few months ago. They took all my points and the funds in my wallet. I contacted Alaska showed proof that the flights were for booked under someone else's name and Alaska re-instated my points/wallet after a few weeks. They froze my account and still I can't make any redemptions though. I need to follow up with Alaska about getting it unfrozen
#10005	07-Jan-25	Reddit	RareLime		Same situation for me as well. I found an award flight to Japan about a year into my account being locked and of course by the time customer service opened the award was gone. They let me remove the PIN step but I had to verbally acknowledge if my account was hacked again I wouldn't be able to recover the stolen miles. I will say the person I was working with was deeply apologetic about the process and rules and helped me file a complaint about it.
#10006	16-Jan-25	US Card Forum	Hourglass 9		I just received an email from Alaska Revenue Protection saying my account was suspicious and I needed to call their customer service. At first I thought it was a phishing email but after checking the phone number I found it was legitimate. Then I logged into my account and saw my points were down to a few hundred a bunch of tickets had been swapped out and my email and phone number had been changed. I waited half an hour for customer service and they said there have been many cases recently including travel agencies of fraudulently using other people's accounts. They told me to upload my ID and set a four-digit password and that I would have to call to unlock it before each use. They also said that if I was fraudulently used again after that they wouldn't provide compensation. :cry: Are there any security breaches lately? I've always used Google Password Manager and I don't think I've ever manually entered my password.
#10007	23-Jan-25	TrustPilot	Maeve		I recently discovered that my Alaska Airlines mileage account was accessed without authorization and my miles were used to book flights under unknown names. While my miles were eventually restored and my account was locked the process was frustratingly slow and their communication was severely lacking. Customer Care admitted they were aware of this ongoing security issue yet there was no urgency in addressing it. When I repeatedly asked when security improvements would be implemented they avoided the question provided no timeline for changes. It's unacceptable for a major airline to downplay a security breach affecting customer accounts. Alaska Airlines must take immediate action notify affected customers proactively and prioritize stronger security measures before more travelers fall victim to this issue.
#10008	28-Jan-25	FlyerTalk	worldwidedreamer		As an additional data point someone hacked into the MileagePlan account of my wife and also redeemed points for Qatar Airways flights. What's strange is that of all Alaska partners it seems like there is a coherence of fraudulent awards booked on QR. Weird huh?
#10009	28-Jan-25	US Card Forum	meteorsin	500,000	My email account was hacked. Following the instructions in the forum I checked my balance from highest to lowest and sure enough it had been stolen. Minus 500000. I think so. I checked my HA account and there were no related records. The customer service line has a two-hour wait
#10010	29-Jan-25	Twitter	adamstatonsmith		AlaskaAir My account was hacked—miles stolen name changed email changed phone number changed and password changed. And now you're telling me that if this happens again you won't refund the miles because you're 'not sure where the responsibility lies?!' 2 hours on the phone and 7 emails later its finally fixed but 'sorry we cant distribute any apology miles because we're not sure it was us.'
#10011	01-Feb-25	Reddit	digitalkyle		Yup. Happened to my wife's account. Using miles is now a pain. I don't understand why they don't implement some sort of 2fa. This is standard security across most sites these days. We got all the miles back and were told 'if we find out this was you. We will peruse prosecution'. Anyhow miles back with having to unlock before using.
#10012	01-Feb-25	Reddit	idkdc1031		Alaska account Hacked :( And they are using my miles. Tried calling their phone number (2+ hours wait) and text message (do not support account issues). Anyone experienced this and what to expect. Does Alaska undo transactions and redeposit miles.
#10013	01-Feb-25	Reddit	no_names_vey123		This happened to me about 6 months ago. They cancelled the fraud transactions and refunded the amount. I also requested a new mileage number and they provided me with a new account. One annoying thing was that every time I use the account from then on (any miles related purchase) I have to call them a provide a code to unlock the account. Otherwise they will not refund any future fraud transactions.
#10014	01-Feb-25	Reddit	FlashyOutlandishness		Just went through this a few weeks ago as well and had the same experience.
#10015	01-Feb-25	Reddit	super_lameusername		Not sure why the downvotes. This is exactly what happened to me as well.

Ref #	Date	Platform	Username	Miles Stolen	Comment
#10016	04-Feb-25	US Card Forum	MegaBrother		I received a Chase transaction notification right after the Chinese New Year. Upon checking I saw my Alaska Airlines account had been used for a zero-dollar purchase. The name seemed to be Indian and the flight was from Dubai to Sri Lanka. The strangest thing is that it used my expired credit card but it still charged the new card even though it was expired.
#10017	05-Feb-25	FlyerTalk	AKLlifetimeFlyer		This just happened to my friend today. The hacker redeemed (or brokered) a CX award redemption (originating in India) with his MP account and spambombed his email to try to hide it. Thankfully AS reinstated all of his miles when he called customer care even though the first leg of the trip was already completed. This friend of mine is no slouch a techie for sure so it can happen to anyone. AS locked his account and gave him a pin to reference. AS also indicated they will be introducing 2FA soon. stay vigilant out there.
#10018	10-Feb-25	Twitter	jdwarenn		Were Alaska Airlines Mileage Plan accounts compromised? Is anyone else missing a whole bunch of miles?
#10019	11-Feb-25	Twitter	NezhatNico		AlaskaAir's policy for verifying my account that was hacked (someone booked multiple flights using my miles) is for me to reply to a customer support email with a phone of my drivers license. No secure link or encrypted file share service. Or I can fax a copy...
#10020	13-Feb-25	Twitter	mauwow		AlaskaAir is anyone working at your contact center? I've been on hold for 1hr and 45 min+ after placing a call and requesting an auto call back. My mileage account was hacked and would like to speak with someone.
#10023	20-Feb-25	Facebook	SP		My Alaska account got hacked also. I am glad to have the points back but the lock is a pain in the ....
#10024	20-Feb-25	Facebook	VW	200,000	Anyone here beat me to this for the first time ever I got screwed by my locked Alaska account because in the past I was hacked and lost 200k points. haha wish I was able to get it got stuck waiting for Alaska to unlock the account for me to book. By the time I got it unlocked gone
#10021	20-Feb-25	Reddit	goodwinebadchoices		I had mine hacked last week. Still (patiently) waiting for them to return my balance
#10022	20-Feb-25	Reddit	crazycouponman	70,000	Another hack story. They need 2fa immediately. Customer service is the worst. So I've heard and read of several people's Mileage Plans accounts being hacked recently with the fraudsters being able to make huge miles purchases - This happened to me last month. I discovered this because a charge appeared on my Alaska card for \$5.60 (usually the taxes you pay for a ticket booked with miles). Someone had managed to fraudulently make a booking worth 70k miles - the scary part is I received no email no text no push at all. The hacker had not even changed the email address on my account Alaska simply does not send the right security notifications out to the email/phone on file if you've made the booking with a different email address (ofc the fraudsters know this). Alaska customer care reinstated the miles and locked my account with a pin - They told me I need to call back every time I need to make a booking with my account locked. Tried to call Alaska (in the pm) for a booking yesterday I had to wait on the phone for 2.5 hours (no option for a call back). Spoke to three of the rudest CS reps I've ever spoken to in my life (they all seem to think they are better than you) they unlocked the account for an hour during which I had to scramble to make my booking. The second time I had to call them (in the am) also waited 30 minutes on the phone. Calling to have to make a booking is not a reasonable option. They also said if I unlock my account permanently and fraud happens again they will not reinstate the miles again. Rather then providing the right online security measure with 2FA they would prefer to threaten and inconvenience their. End of my rant - I used to think Alaska was one of the best airlines but it has quickly shot down to the bottom. Hope this helps someone - I did not realize miles would be so easily hacked in 2025 keep an eye out and change your passwords regularly. Feel free to post your Alaska hacked rant below and to put some kind of pressure on them not that they care at all
#10025	20-Feb-25	Reddit	Zakarumae		Happened to me yesterday but they changed my email to a new domain but kept the beginning the same. Weirdly they booked me a flight along with the scammers. Only caught it because like above I get texts every time I have a charge on my card and they used my Alaska card along with the miles. Along with 2FA I'd love a secure site to upload the government ID to as well instead of sending it in an email. The other surprise was them signing my real email up for a shitload of spam emails to flood my inbox but why I don't know. I never even got an email about the miles being used or the flight booked notification since they changed the email address.
#10026	20-Feb-25	Reddit	No-Fig-8614		I got hacked luckily they caught it and froze my account and gave me back my miles but had to go to my CC company to get the refund on the on file. How DO THEY NOT HAVE 2FA?!
#10027	21-Feb-25	Reddit	Eggta1onn		I was hacked two months ago and I'm still waiting for my wallet funds to be returned.
#10028	21-Feb-25	US Card Forum	ghtjyiy	600,000	This is the first time I've been hacked. It involved Alaska miles they bought three tickets—two in Indian names plus my own—on Qatar Airways from TRV in India to Doha (DOH) and then to Toronto (YYZ) with each ticket costing 200000 miles. My points were immediately refunded after the call. I saw that others who had been flying for a long time also got their points back after the call which is great about Alaska. The only downside is that the account gets locked and I have to call to temporarily unlock PIN each time I want to redeem.
#10029	22-Feb-25	Reddit	MrGutterballs	85,000	Same exact thing happened to me. 85k to reserve a hotel in Spain. Took a bunch of work to get it reinstated too. And then the PIN garbage.
#10030	03-Mar-25	Facebook	SPH		I just randomly opened my Alaska Airline account and realized that someone named Andre Benson got himself two business class tickets with my mileage. He reserved yesterday and he is flying right now on a second flight. Trying to get help to catch him but what do I do?
#10031	03-Mar-25	Facebook	BRC		Someone hacked into my credit card account and wiped out all my points last year. I got them all back but I did not know this was a thing until then. Reading these comments seems like it might be common...yeesh!!
#10032	03-Mar-25	Facebook	BA		It happened to me before but I noticed it the day before they were supposed to fly out so it got canceled. I'd call the airline asap.
#10033	03-Mar-25	Facebook	EC		Happened to me a few weeks ago. Alaska locked down my account immediately placed a flag on the person's flights and refunded my points after I sent over a copy of my license. Took about 45 minutes for the entire process.
#10034	03-Mar-25	Facebook	EN		Omg it happened to me too last year. But I was able to cancel the flights before he took em. And got my miles back. Smh scammers. Gluck
#10035	03-Mar-25	Facebook	LB	500,000	our Alaska Airlines account was hacked as well 500000 miles for a hotel in Canada. We did not have to make a police report and they refunded our miles after they did their investigation. I don't know if their policy has changed.

Ref #	Date	Platform	Username	Miles Stolen	Comment
#10036	03-Mar-25	Facebook	VC	80,000	That's so strange I logged in to check my balance after reading this and am missing almost 80K miles with no redemption and activity. to update they say someone issued a BA ticket on my account clearly not me. Someone from Ghana flew and Alaska doesn't even e mail when a ticket is redeemed - what a massive idiocracy. Please check your accounts I checked mine for missing miles- reached out to Alaska and turns out some Richard travelled on my Alaska points on BA in September on Business Class.
#10037	03-Mar-25	Facebook	GH		Unfortunately happened to me too. First call Alaska and start a case. They were able to refund all my points but I have a permanent lock on account which I can only temporarily unfreeze with a pin given to agent verbally. Unsure why they don't have 2 factor still lol Also probably a good reminder to stop recycling the same password and use some type of password service like Bitwarden. if they got into one account with their password I'm sure they're trying to get into tons of others
#10038	05-Mar-25	US Card Forum	wsyzxlz		My account was hacked without any notification. I only discovered my points had been stolen when I logged in and by then the flight had already taken off. Did you get your points back in the end?
#10039	06-Mar-25	Facebook	JK		This happened to me before I even received the card in the mail or created an account. Not sure what's going on with Alaska.
#10040	06-Mar-25	Facebook	MD	100,000	DP: Not sure if this has been posted before. Apologies if redundant. My Alaska acct was hacked and they charged \$300 in flights and took 100000pts. Everything was recovered but now I have to have a PIN number and call in to Alaska customer care if I want to use my miles. This has to be done during business hours and they are not open Sundays. They offered to not have the PIN etc but then said if miles were stolen again they would not replace. I waited 20m on hold to speak with customer care so I assume that's probably going to be average just to tell them I want to book an awards flight in the future. 1. The flights that were booked with the points had not happened so the points weren't spent. 2. Authenticator app 2 factor text or emails are apparently not an option 3. Maybe this is a post for travel grumps but I just built up a bunch of Alaska miles and now this little wrinkle is going to be an unnecessary headache. 4. I am grateful to get the miles back but I won't be snapping up any hard to get seats without a massive hold time to customer care that occurs sometime bt 9a-6p Monday - Saturday . Rant over. Anyone else had this happen?
#10041	16-Mar-25	US Card Forum	DaDouDou		Update: The Mileage department was closed on Sunday so I called to make the reservation and left a callback. I received a callback two hours later. I explained the situation and customer service said they would check with their staff to see which transactions were fraudulent. They said they would send me an email within 24 hours asking for my driver's license to prove my identity and then they would send me a PIN. They said I would need to call and use this PIN to unlock my account before making any future redemptions. we will redeposit your points to your account after the verification. Just found out I've been infected. I searched through the barrage of emails from the past few days looking at various hotel companies and their points/reservations but I didn't find any suspicious emails so I ignored them. Then I just saw the credit card notification and realized that someone had charged me 5.6% in taxes and that's when I realized I had really been scammed. I was surprised to see that it was an Alaska flight and then I realized that someone had already redeemed a business class ticket for YYZ - DOH - TFU (this is amazing you can't cancel on Alaska and you can't even see the Qatar Airways schedule or reservation number). I can see the contact emails casaplanyacht.ocn.ne.jp but they seem to be fake. Why didn't I receive an email notification about the points redemption? Chat support said they didn't have the authority and told me to call back on Monday. I'll talk to them on Monday. There was also a BOS - SEA redemption that happened this afternoon which was Alaska's own service but I canceled it. Judging from their names they all seem to be Chinese. I'm wondering if I should send them an email telling them to stop buying tickets from ticket agents. Please be careful with your security. Don't use simple passwords for your Alaska account (mine was indeed very simple and it had been compromised before it was found through a credential stuffing attack using your email address and password).
#10042	16-Mar-25	US Card Forum	Spacetime		Me too. It's so troublesome. I can't redeem it outside of working hours. During working hours I have to wait in line for half an hour for customer service and then it only unlocks for one hour.
#10043	16-Mar-25	US Card Forum	YanamiAnna		Without OTP IT is truly terrible. Alaska even created a separate email service. Once your account is hacked you can only lock your customer service PIN which means you'll miss out on mileage tickets and your account is essentially useless.
#10044	16-Mar-25	US Card Forum	Fly Away		Hopefully I can get my mileage back from hitting the teacher tomorrow. I was so scared that I quickly changed my password to a string of random characters longer than 20.
#10045	16-Mar-25	US Card Forum	Irish Coffee		I was indeed too lazy. I thought that since there would be an email notification the credit society could just dispute it immediately. Unexpectedly there was no email notification.
#10046	16-Mar-25	US Card Forum	Isroyce		Last month my account was also hacked. They used it to book an Alaska Vacations trip in Brazil through Expedia but deducting Alaska points. I received an email and contacted Alaska immediately but they said the trip was non-refundable and I had to call the hotel to cancel. I told them that since it was fraudulently used I couldn't cancel directly and they said yes I had to contact the hotel (scumbag Alaska). Then a while later they told me the hotel staff handling this had gone off duty and I had to contact them again tomorrow (seriously I want to curse Alaska). Unexpectedly Expedia called three times (I missed the first two) asking if I had booked the trip. I said no it was fraudulently used and Expedia canceled it for me and my points were immediately refunded.
#10047	18-Mar-25	US Card Forum	nate1874		Just now during my routine check of all accounts I discovered that 150000 RMB had been stolen from account AS and five tickets from Hawaii to Seattle for tomorrow had been purchased. I immediately changed the password and canceled the tickets.
#10048	30-Mar-25	US Card Forum	harryiori		My Alaska Airlines account was hacked before. I called customer service and they refunded my deposit. Then they asked me to send the front and back of my ID and a setup PIN. They said if I didn't get the setup PIN they wouldn't refund my deposit next time. The key issue is that after getting the setup PIN award tickets can only be issued by phone and not 24/7. Alaska Airlines Customer Care Phone: 1-800-654-5669 7:00 am - 7:00 pm (PT) Monday-Friday 8:00 am - 5:00 pm (PT) Saturdays This is basically a total rip-off. It's clearly their problem that the account was hacked so why should the consumer have to pay for it? I'm absolutely furious! Is there any way to get revenge?

Ref #	Date	Platform	Username	Miles Stolen	Comment
#10049	22-Apr-25	FlyerTalk	Cupajoe	210,000	I discovered when looking at my Milage Activity on April 12th my account had been breeched. Six passengers four being children (the oldest child being 10 and two infants). The flight was from Quebec I believe to Dubai on Qatar. My activity shows six awards withdrawn on March 3rd and redeemed and flew March 5th. The award redemption is inside the required 72 hours allowed by AS which would make it impossible to issue but whatever. Partner airlines prob. have diff. requirements. I did not receive any email or phone call from AS of suspicious activity at the time of the withdrawal. Each one way award Was 35K miles x 6 passengers = 210000 miles. On my activity I can see the name of the passengers. I called over the weekend April 12th to AS CS which was closed as it was after 7 pm pacific time. The rep. was kind and compassionate and while not able to remedy situation she spoke of similar methods to be made whole on miles stolen. She forwarded the info to I think the fraud dept. and she told me to write an email with the data I knew. I wrote that on Sunday so I suspect I should reach out to my MVP gold milage rep. The rep explained that the magnitude of AS site evolving has left exposure to many. AS is always kind to me so I feel confident that all will be fine. Wish there wasn't PIN restrictions put on all of us who have been breeched but out of my control. I keep a fairly extensive password management and obfuscation but they got in regardless. More creepy is they listed my daughters name who has her own CC and MP as the initiator of the transaction. And then put a completely random address for her in Juneau AK. Who knows the hackers seem to be always ahead of the institution holding the data. Hopefully it will all get sorted out. *Further research indicates credit card charges (\$94.76/passenger) not refunded - told to contact bank.*
#10050	24-Apr-25	LinkedIn	Elliot Rosenberg		Mileage Plan hacking I discovered last month that my Mileage plan account had been hacked in December. Guy stole my points and bought tickets with it. I hadn't noticed until March because I hadn't flown Alaska in that time frame. I did all the things and had my miles restored and dutifully changed all passwords. I purchased some tickets a few weeks ago. Today I tried to check my account to verify something and once again can't access my account and get a we don't have any account linked to this email response when I try the Forgot Password option. This is exactly what happened last time so Im assuming I was hacked again. 2 questions: 1. Considering I did all the security things right and I haven't had any problems with any other accounts does this seem like the breach is more likely coming from their end? I find it hard to believe that someone who has access to my accounts is choosing to only steal my Alaska miles. 2. How does this scam work? You need to present ID to fly- how do they not catch these people after the fact? It's not like there's a secondary market they can sell tickets to. Obviously I'm missing something here would appreciate if someone can enlighten me.
#10051	05-May-25	Reddit	ensorized		Mileage Plan hacking I discovered last month that my Mileage plan account had been hacked in December. Guy stole my points and bought tickets with it. I hadn't noticed until March because I hadn't flown Alaska in that time frame. I did all the things and had my miles restored and dutifully changed all passwords. I purchased some tickets a few weeks ago. Today I tried to check my account to verify something and once again can't access my account and get a we don't have any account linked to this email response when I try the Forgot Password option. This is exactly what happened last time so Im assuming I was hacked again. 2 questions: 1. Considering I did all the security things right and I haven't had any problems with any other accounts does this seem like the breach is more likely coming from their end? I find it hard to believe that someone who has access to my accounts is choosing to only steal my Alaska miles. 2. How does this scam work? You need to present ID to fly- how do they not catch these people after the fact? It's not like there's a secondary market they can sell tickets to. Obviously I'm missing something here would appreciate if someone can enlighten me.
#10052	12-May-25	US Card Forum	tlitb		It was also stolen.
#10053	14-May-25	Reddit	mutt82588	250,000	This just happened to me. Someone got in my account changed the recovery email and phone number and booked a ticket on qatar airlines JFK to hong kong for 250k miles. Must have got a sick seat. Did not get notified by AS that things were changed. I had not changed that password in many years so probably found in data breach. Alternatively I'm wondering if some one had spoofed the link for to transfer hawaiian and alaska miles and i accidentally entered it there. At any rate only found out when I could not log in to my acct. Called to day and AS was very helpful froze everything and told me that the flight hasnt flown yet so they are going to claw my miles back. The CSR said that unfortunately she has to do this 3-5 times per day and if the flight has already flown then miles are gone. I asked if I should report to authorities adn she told me not to even bother. On my milage history it had the passengers name and the qatar confirmation number. I tried to look up the reservation on qatars website but the itenerary was already cancelled. My question is why doesn't the airline go after these folks? Seems like this is a rare category of internet fraud where the fraudster or associate has to use a real identity and has physically show up somewhere. They come to you in a heavily policed secured area! If the airline didnt cancel the ticket flagged it internally and then just had it error at boarding with an airport cop right there boom. What am I missing here?
#10054	03-Jun-25	OneMileAtATime	RobASFO	170,000	Ben I too had miles stolen from my Alaska account for a Qatar business ticket Montreal issued to a woman in Lagos Nigeria. I too tracked her down on social media called Alaska to give her name and stated that these were stolen from my account. Alaska reinstated the 170000 miles to my account and I now have a PIN number to access the account just like Ford Although this was caught two days before the actual flight and I would suspect that Alaska nullified the ticket I asked Alaska how they could issue a ticket under a different name and gender with my frequent flyer miles but did not get a satisfactory answer. In fact I didn't even get an official acknowledgement in the form of a letter or email let alone an apology. It's strange but I doubt companies go after these individual scammers as it is too hard to prosecute unless it's done on a Federal level. A lot of the identity theft stems from these criminal gangs in places like Nigeria and Russia.
#10055	03-Jun-25	OneMileAtATime	Nedskids		I had a similar thing happen with Alaska a few months ago and have the same PIN/call/unlock thing. Which is only annoying when you're trying to get a mileage ticket in a hurry on a weekend when another airline has gone IROP... I had to resort to flying Southwest cross country this weekend.
#10056	03-Jun-25	OneMileAtATime	sowestcoast	59,000	This happened to me. Two different individuals redeemed my Alaska miles on two American Airlines flights totaling 59000 miles. I googled their names and found their FB profiles (also seemingly Nigerian?) and was tempted to confront them as well. Seems like there is some loophole that folks have found with redeeming partner awards? I now have to call Alaska to unlock my account each time I want to redeem a flight with miles.

Ref #	Date	Platform	Username	Miles Stolen	Comment
#10057	03-Jun-25	US Card Forum	Aubonpain	215,000	This morning I discovered I couldn't log into the app which seemed wrong. I reset my password and found that neither my email address nor my phone number was recognized so I immediately called. After waiting 35 minutes I was finally able to speak with the agent. The perpetrator purchased the ticket in May a Qatar Airways business class flight from JFK to BKK using 215k points. The ticket has already been issued and the flight completed. The passenger's name is Lin Mei.
#10058	04-Jun-25	US Card Forum	chowchan		My AS account was also hacked and tickets were sold to an American in Austin. I didn't find out until several months later. I called customer service to get my points back and the account locked. Miles can be used to log in but to log out I have to call to unlock it which takes two hours. I think it's a bit troublesome but it's safer this way. I didn't receive an email about the ticket issuance and my email address wasn't updated after logging into my account. It's possible the email address was changed back after the ticket was issued.
#10059	04-Jun-25	US Card Forum	tlitb		My AS was stolen a while ago and it's gone. I contacted customer service and they sent me my ID. They said they would reinstate my miles within 15 business days and also asked me to set a PIN saying that I would need to call every time I used the miles. They said that's ridiculous.
#10060	16-Jun-25	Reddit	ElonFanboisSuck		I was hacked last week though partially it's my fault. The password was involved in a data breach a while back and I forgot to reset this one. My bad on that. Sometimes you get lazy using a password manager and never paying attention to what the password actually is... However I don't understand how any modern web service does not require two factor authentication before changing critical information like password email and phone number. Like it's truly unacceptable at this point for any website especially one as important as air travel.
#10061	16-Jun-25	Reddit	pdxcouplese		I think I'm done with Alaska. A few months ago I noticed new emails and phone numbers on my profile and an international award travel ticket. I called Alaska and the award travel hadn't happened yet so they could reverse it without issue. I updated my password to a long and difficult password. This morning I was sitting in a meeting and all of a sudden two emails pop up saying I canceled two upcoming flights booked with reward travel again. I immediately changed my password again. My account has the feature where I have to call to unlock for reward travel after the last hack so they were unable to book. Alaska won't undo the cancellations. Frankly they won't do anything. Their app is insecure and if something happens they refuse to help. Now I'm on hold waiting to get my account unlocked so I can rebook. The first flight costs more now. I'm shocked at how little they can do and how much no one wants to help. I expected a lot more. Delta anyone? They said both times it came from the app. My phone was sitting next to me when this happened.
#10062	17-Jun-25	OneMileAtATime	MelissaGuest	100,000	It looks like I am in good company. I just tried logging into my Alaska Air account and my password would not work. I then sent in a request to reset my password and I was asked whether I would prefer instructions go to my email address or my phone number (neither of which were actually MINE someone had hacked and changed them!). I called customer service (which took an hour to get through) and after several hours I was able to get everything restored. Someone had cashed in 100K worth of miles!
#10064	17-Jun-25	Reddit	Intelligent-Bat-1521	80,000	Had my Alaska miles stolen in June 2025. But I don't use AwardWallet. Also have unique passwords for each of my accounts. So is a Alaska Airlines breach. Someone transferred 80k miles to Qatar Airlines in the name of Ling Ms Yi. Still trying to get my miles back with Alaska Airlines. They still haven't sent me info on PIN etc. Really wish Alaska Airlines would go to 2F or multi-factor authentication too. Also wish for those accounts affected we were given extra miles & not penalized by having to call in with a PIN in order up use or transfer miles. Hope they have a special call center setup.
#10063	17-Jun-25	US Card Forum	rad		I discovered my account was hacked today. I can't log into Alaska and resetting the password also shows an information mismatch. What should I do?
#10065	27-Jun-25	FlyerTalk	calguy77	300,000	Check your accounts!!! Hack with HA someone tried to steal my AS miles Woke up to an email saying my mid-july flight was cancelled. When I went to the AS website to check. My flight was gone from Trips and in its place was a reservation from NRT to ATL. 300000 miles of mine were used to purchase the flight. Name was Yuan Zhang who booked it. Chatted with an agent and they said I had to call in to block my account. Hold time 4 hours right now.
#10066	28-Jun-25	LinkedIn	Kathy Burkle		Also happened to me - Alaska Airlines
#10067	30-Jun-25	Reddit	ktdiggs		It happened to me too they had me set up a pin to lock/unlock the account. Now every time I want to book with miles I have to call in and wait on hold for X amount of time for them to unlock my account so I can book. If I didn't set up a pin and I got hacked again they wouldn't refund the miles.
#10068	01-Jul-25	Reddit	DefiantCut1460		Account got hacked and the hacker used miles on a trip. I called Alaska and cancelled the transaction and am in the process to get my miles back. Edit: I also changed my password to a strong one! Other than that what would you do?
#10069	01-Jul-25	Reddit	itsendy		Same with me. It's pretty annoying to wait for an hour before you can book and won't be able to call and unlock the account when it's during customer services's off hours
#10071	02-Jul-25	Facebook	JM	200,000	I just got stolen 200k+ miles from Alaska don't forget to randomly change password. Alaska refund my miles and have to setup a pin for future award booking. I got an email from Alaska about suspicious activity on my account and need to call them
#10073	02-Jul-25	Facebook	JL		ht happened to me 2 now i could only redeem by calling in with pin
#10074	02-Jul-25	Facebook	JRM		his happened to me too. Why I would want to book a flight in someone else's name from South Africa to Nigeria I think it was is beyond me.
#10070	02-Jul-25	Reddit	Andyh10s		Most likely a data breach. I had my account hacked on Monday was able to recover the miles as well. Seems to be a lot of these reported with the points transfers and also apparently a large data breach a few weeks ago

Ref #	Date	Platform	Username	Miles Stolen	Comment
#10072	02-Jul-25	Reddit	pointstopointb	500,000	AwardWallet Saved Me From Having 500K+ Alaska Miles Stolen I got an odd notification from AwardWallet just now that my Alaska Airlines mile balance had gone down by over half a million miles. I found out that someone had hacked my account and booked two business class one-way tickets that were leaving within eight hours from the US to Doha to China. Fortunately AW gave me the confirmation numbers and I was able to cancel the tickets and reclaim my miles. I also was able to change my password. I'm on the phone right now with Alaska and on line to Qatar to report these thieves and give them information. My guess is that my information has been compromised for a while (last changed password in 2024) but because I had recently moved Amex -> Hawaiian -> Alaska my account became useful for them. Heads up to change your passwords.
#10078	03-Jul-25	Facebook	CK		Happened to my wife just the other day. Alaska locked the account refunded the mileage and put a pin on it. 2 factor MFA would be helpful for everyone as annoying as it is.
#10079	03-Jul-25	Facebook	VR		This happened to me scammers booked a hotel stay with my points. They sent like a hundred spam emails right after so I wouldn't notice. Alaska got me my points back but it's a pain in the butt to call customer service every time I have to unlock my account so I use my points. I don't think they have two factor auth.
#10076	03-Jul-25	Frequent Miler	Amol	500,000	Check your Alaska Airlines account security — I almost had over 500,000 miles stolen today! Today I got an AwardWallet notification that my balance went down by over 500,000 miles and that there was an upcoming reservation on it. Someone had taken my miles and booked two people a last minute business class award on Qatar from the USA to Doha to China. Luckily I had about 7 hours before check-in so I immediately called Alaska Airlines but there was a 1-hour wait. I was able to log on to my Alaska account and cancel the tickets and get my miles back then change my password. I finally got a call back from Alaska 2 hours later and reported the reservation details. My guess is that someone has had my account information for a while but in the past 2 weeks I have transferred Amex to Hawaiian and pooled all my family's Hawaiian/Alaska miles into my account — with the inflated balance my account was now able to book multiple partner international business standard level mileage awards. I didn't get a single notification from Alaska — not an email app notification or 2FA (which they don't have). I urge everyone to check your Alaska password security and consider changing it particularly if you have a large inflated balance.
#10077	03-Jul-25	Frequent Miler	Stephen Pepper	85,000	I'd encountered this same issue myself although my experience was just over a year ago. I'd gone to book a couple of business class tickets from the US to the UK in May only to find my account with a very low balance. At first I was kicking myself thinking I'd let my miles expire. However when checking the activity on my account I noticed that there were three Mileage Plan Hotels redemptions all on the same day in February. Based on other reports from people whose accounts were hacked the redemptions that take place are last minute bookings usually for premium cabin flights. The reasoning for that is that it gives less time for the legitimate account holder to notice the missing miles and have those reservations cancelled. On my account rather than booking premium award flights someone made several hotel bookings presumably last minute for Valentine's Day. I didn't notice these redemptions until a few months later so it was too late for me to cancel those redemptions. I reached out to Mileage Plan to report that my account had been compromised and that someone had redeemed the majority of my miles. They offered to reinstate my miles provided I could provide a copy of my driver's license or passport showing my legal name along with a four digit PIN to secure my account in the future. Those documents could be mailed faxed or emailed so I emailed them over to speed up the reinstatement of my miles. In the meantime I changed the password on my account. It took a full week but Alaska did eventually reinstate all my missing miles which I appreciated.
#10075	03-Jul-25	Reddit	rhefter		Same thing happened to me. I now have a block on my account for any award bookings. I have to call in to get it unblocked. The reps will stay on the phone while you are booking and then lock it back up right away after you get the confirmation. It's honestly not that bad and considering they do not have 2FA I'd rather the block be on my account.
#10080	04-Jul-25	Facebook	AR		Same thing happened to me. They cancelled the fraudulent flights and my legitimate flights. It was a mess! Now I have to call Alaska directly to book any award flights.
#10085	09-Jul-25	FlyerTalk	my321	500,000	Someone booked two close in tickets to Japan with my Alaska Airlines miles. Alaska Airlines allowed someone to enter new names and send the only confirmation to an Email address of their choosing. I never received an Email text or phone call from Alaska Airlines about more than 500K in miles being used. If it wasn't for the coverup I would not have known about the fraudulent bookings until long after the flights were taken. When I woke up to roughly two thousand SPAM emails from a small number of addresses I guessed that the attack was designed to cover up something. Since I use multiple email addresses it didn't take long to guess that it was an airline. Alaska Airlines was my first choice. I was able to cancel the tickets and change the confirmation Email address to one of mine. I use a unique password for Alaska Airlines and my Hawaiian Airlines password does not resemble my Alaska Airlines password.
#10081	09-Jul-25	Frequent Miler	NYCHoo		Exact same thing happened to me and had to go through same process afterward. FYI Alaska Mileage Plan service desk is NOT open on Sundays so you can't unblock your account on Sundays.
#10082	09-Jul-25	Frequent Miler	AlG		My account was also hacked 2 weeks ago....it's been a week since I sent in all the documentation but still no movement on my account....I called Alaska and they said they are really backed up so I'm assuming you're right and this is happening a lot lately.
#10083	09-Jul-25	Frequent Miler	Patricia		This happened to me today. Luckily I was checking my account frequently due to an upcoming trip and was locked out so I immediately called. The person had booked a flight and checked in but the flight had not boarded. I so hope they arrested the person.
#10084	09-Jul-25	Frequent Miler	Kevin		Same thing happened to me about a month ago!
#10086	09-Jul-25	Frequent Miler	Mark	200,000	Luckily in my case Alaska noticed suspicious activity on my account and emailed me regarding it on May 29th. Someone with a Chinese name had booked business class tickets costing over 200K miles — and changed the email on my account. So folks should double check their account email as well. Eventually reinstated with the aforementioned process and PIN lock on my account.
#10087	09-Jul-25	Frequent Miler	luckystan777		Thanks for the alert. Just checked my account and their was 2 1st class tickets booked from TPE to LAX. Cancelled them and changed my password. Thanks
#10088	10-Jul-25	Frequent Miler	L D		Happened to me too a month ago
#10089	10-Jul-25	Frequent Miler	Dante		Just dealt with this yesterday

Ref #	Date	Platform	Username	Miles Stolen	Comment
#10090	11-Jul-25	Frequent Miller	Pippa	85,000	Yikes! I also just found out that I had 85000 miles stolen transferred by a Ying Ms Li to Qatar Airlines on June 17. I was only just made aware of this. I keep trying to change my password on Alaska Air app & website but the only way to change password is to log out & select forgot password. But when I do this I get a system error. Alaska Air says they can reinstate my miles but I have to agree to email my ID create a PIN (still don't know how to do this) & going forward only use their phone line to ever use the miles or transfer the miles. Their phone lines have massive wait times! Hours! If I ever find a mileage deal it will surely be gone before I can get ahold of someone on the phone. Alaska Air offered no apology. No accountability for this breach. Will FTC do anything? Why doesn't Alaska Air have 2 factor authentication? How long has Alaska Air known about this? Why is Alaska Air putting blame & weight of this on their customers? (I don't reuse passwords nor share my info) Would love some help & accountability.
#10091	12-Jul-25	Facebook	AHL		Someone hacked my Alaska mileage and currently enroute from Dubai to Houston via Qatar airways business class. How do I report this or even better get them arrested if possible. They're not anticipated to land until after 4pm? Tia
#10092	12-Jul-25	Facebook	CY	400,000	Alaska doesn't have 2FA and I think this fraud is committed by their employees. My friend has a long password with 400000 points stolen. Fortunately he caught it before flight took off and got his points back by calling Alaska. Good luck.
#10093	12-Jul-25	Facebook	EI		Same here . Called Alaska before flight dept and canceled the hacker's award
#10094	12-Jul-25	Facebook	ML		Same thing happened to me in March they ended up booking like 16k of flights Amex got my money back. Super weird because the booked like 8 flights all in my name going all over the world
#10095	12-Jul-25	Facebook	RNS		Different scenario but similar. My points we used to check into a resort in Mexico. However I got the alert the minute they were accessed and called. The cc company was talking to resort to cancel as the ppl tried to check in. I was on the call and could hear it all. It looked like the ppl trying to check in for their fabulous weekend had been scammed too.
#10096	12-Jul-25	Facebook	RP		I too have gotten my Alaska account hacked but instead they bought tickets with a cc saved to it. I'm never doing that again.
#10097	12-Jul-25	Facebook	RS		I had the same thing happen to me recently. I reached out to Alaska support on 82008 over text and they help me out quickly.
#10098	13-Jul-25	Facebook	LDA		Ugh. This happened to me recently. Luckily i caught it before the flight. They reinstated the miles but now I have to call and unlock my account everytime I want to use my miles to book a flight. So much for those getaways to Tahiti that you have to jump on immediately
#10099	13-Jul-25	Facebook	LA		This happened to my FIL about a month ago. Only caught it because I was helping them book an award flight. Alaska said there's some scam where they take peoples money to book them a flight they use some random unsuspecting person's miles to actually provide the ticket and pocket the cash. Wish they would add 2FA to their loyalty accounts instead of this pin and rep booking requirement.
#10100	19-Jul-25	Facebook	WB		Keep an eye on your Alaskan accounts. Mine was hacked. Spoke to the rep today and she said they had a huge influx since the Hawaiian miles transfers started especially since the end of June. Someone booked Doha to Toronto Qatar Business class with mine. I missed it by 12 hours he flew yesterday so I couldn't even get any joy out of stranding him at the airport. Also they said they will only return points for fraud once. If it happens again they may not.
#10109	19-Jul-25	Facebook	VB		This just happened to me a few weeks ago. I contacted Alaska customer service had to verify my identity and they immediately put the miles back in my account. I only noticed because I was booking a flight and a weird email populated for the confirmation. That triggered me to look at my miles then booked flights and someone had booked a flight from LAX to ATL. The name was in the booking. It was a washed up has been rapper lol. But moral of the story easily handled by customer service
#10101	19-Jul-25	Reddit	goa_to_rio		Sorry to hear about that. Stressful garbage for no reason if you ask me. Happened to me 2 months ago. To use any miles now I have to go through this jank process of calling in unlocking my account with a verbal pin to then have the account unlocked for booking for 1 hour. Sucks.
#10102	19-Jul-25	Reddit	jbuzolich	200,000	Yep same with me over 200k miles lost about a year ago. Alaska later restored which I'm thankful for but now I have the pin. We just returned from family trip to Hawaii. The prices were low and I would have preferred to use our existing companion voucher first and then maybe miles on the other ticket. My wife insisted we burn down the miles instead since there's no faith anymore they will still be available next time. They really need to up their email communication and add 2fa at minimum. A big part of what upset me besides the lost miles is that the flights the awards were used on were not in my family name of course and not between cities or countries I have ever been to. It should have easily been flagged as unusual.
#10103	19-Jul-25	Reddit	lisariley2	300,000	I had 300k miles stolen and Alaska gave them back to me and I now have a PIN number. But I'm ok with that as I don't want anyone to steal my miles. The person stealing leaves so much personal information it makes wish they would get charged for stealing. It seems like it would be pretty easy to catch them. I do know that the person stealing is not always the person traveling. But still
#10104	19-Jul-25	Reddit	meowsabbers	250,000	Just noticed I had 250000 miles fraudulently redeemed from my Mileage Account Like many of you I transferred American Express points to Hawaiian Airlines and then to Alaska Airlines just days before the transfer partnership expired. In my case I transferred 270000 American Express points. Since then I hadn't really had a need to log in to my Alaska account. I happened to be searching for some flights today and noticed I had about 30000 miles in my account. I thought that was odd and then looked on Hawaiian Airlines. Sure enough my transferred miles were not there either. I then checked my mileage activity on Alaska and saw that on July 4th 250000 miles were redeemed for a flight from HNL to JFK. I live in LA and the name attached to the reservation was definitely nobody that I know. I spoke to Alaska and they confirmed that they flight was in fact flown but did clear this up quickly and reimbursed my account with the 250000 miles but I was a little taken aback by the way they were basically saying this is my fault and not theirs. It's a little crazy someone can redeem any amount of miles and the account holder is not notified. They said this reimbursement would be a one time courtesy and that if I don't add a PIN to my account as an additional layer of security they would not be reimbursing me if it were to happen again. I of course opted for the PIN but the downside is if I want to book reward travel I can no longer do it online or on the app I would have to call and book. Got the miles back quickly but I nearly lost my stomach for a minute there. Stay vigilant!
#10105	19-Jul-25	Reddit	Specific-Rip4123	60,000	Happened to my husband just recently. Thankfully he got back the 60k. When we logged in to his account we saw the names of the an entire family their address they tied to his account and their cc. Crazy!!!

Ref #	Date	Platform	Username	Miles Stolen	Comment
#10106	19-Jul-25	Reddit	Ok_Sir_7220		This happened to me but I noticed before they used the miles. It's a huge pain to have to call and have the pin removed each time but I do it for safe guarding my miles. It's crazy to me they don't have any safeguard about your info being changed. I got no email or any notification when it happened.
#10108	19-Jul-25	Reddit	MozzarellaBowl	220,000	Same here. 220k miles from Saudi Arabia. Extremely frustrating and stupid of them. Why wouldn't I at the very least get an email notification about this? Apparently what they typically do is steal it as a travel agency do the person using it paid them a third party and has no idea it's even illegitimate (apparently) and makes it harder to find the actual criminal. That being said I blame Alaska for making it stupid easy to steal.
#10107	19-Jul-25	Twitter	friendly_jen	100,000	Something I never expected happened today. My AlaskaAir account was hacked and over 100k miles were used to buy a round trip business class airfare from London to DC. I have a name but blasting that will probably do nothing. But wish they could have some real repercussions!!
#10110	20-Jul-25	Facebook	RG		this happened to me last week be vigilant
#10111	20-Jul-25	Reddit	Opposite_Clock_1587		This happened to us too! It's such a pain using the pin but they said if we didn't use the pin and it happened again we wouldn't get the miles back.
#10112	22-Jul-25	Reddit	Acceptable_Bus5038		Happened to me Saturday morning. I was able to catch it cancel the flight and get my miles back before they email bombed me. What I was unable to do was change my password without calling them which was concerning. They told me it's a glitch that they having sometimes. I was supposed to receive a call back but haven't yet.
#10113	22-Jul-25	Reddit	EarthBanger		Completely agree. Last year Alaska called me to inform me someone used my miles to fly Goa to Doha to Dulles on Emirates in First Class. The flight had already landed in DC and the person was gone. They booked their ticket 90min before its departure. Absolutely crazy there are no secondary checks especially for tickets being booked so close to departure or from a place or with a person that's nowhere on your account. I now too have to call the reservations line anytime I want to use my miles for booking. Super fun since the reservations line has banker hours and no weekends. Extra super double fun when you do your research for reward flights make the call to reservations to have them released for a period of time and then find out those flights are just phantom inventory... Stay safe out there
#10114	22-Jul-25	Reddit	TranscontinentalTop		PIN via email! I don't trust that. Email is not secure. Why isn't email secure? And a text message is? What are you doing with your email account to make it untrustworthy? I'd far rather have a code go to email where I can use an authenticator app and a ridiculous password than get something by text to a number that seemingly anyone can walk into T-Mobile with a halfway decent fake ID and steal.
#10115	22-Jul-25	Reddit	carlabena		Just got my miles stolen. My miles are stolen. I call Alaska. They want me to verify all sorts of personal information by email. While they did not verify shit for the criminal who stole my miles. What a business model. I wonder if I can sue. It's 2025 and they just have single credentials. No multifactor authentication. Now they want me to call every time I will make a transaction with them in the future. Pay for an IT consultant and get your shit together. End rant.
#10118	23-Jul-25	FOX 13 Seattle	JH		Julie Horgan said she first realized something was wrong when her inbox filled with cancelation emails from Alaska Airlines. I started to panic a little bit because I was like no way what are the odds? Horgan said in an interview with FOX 13 Seattle. But it wasn't just her travel plans that were disrupted. I thought it was just my flights being canceled — and [the agent] was like yeah your miles are all gone. According to Horgan someone gained access to her account canceled her booked flights then used her accumulated miles — likely reselling them to someone else on a third party site.
#10116	23-Jul-25	Reddit	mgsp		Same thing happened to me two weeks ago. All they asked for was a photo of my drivers license. Took a week. I set a pin number now. Make sure to go in and erase all the hackers contact info. I just emailed them. You could probably call them. They said if you didn't set a pin and it happens again you don't get the points back.
#10117	23-Jul-25	Reddit	Full-Policy705		I had my miles stolen a year and a half ago. They restored them but I need to call every time I want to redeem them and if it ever happens again they will not reimburse.
#10119	23-Jul-25	Reddit	Zestyclose_Pool_1856		I just had this happen to me too. Someone got into my account and booked business class tickets on Qatar. I quickly changed my password and cancelled the flights. Miles were refunded immediately. From other people's experiences with this it seems like reporting this to Alaska won't solve anything and just becomes a hassle for me. Time for 2FA Alaska!
#10120	23-Jul-25	Reddit	amdinizo	300,000	This actually happened to me too. Some dipshit used like 300k miles to book an economy ticket from India to Canada on Qatar (lols). Luckily I caught it like a day after the booking and changed everything. I think Alaska was part of the data breach that happened a few months ago. Yea they were more concerned about having me talk to their privacy team to protect others vs anything else. They were actually very understanding with me too. This isn't actually an LOL. So they only took 300k of my miles but I did some re-jigging with trips after since I already hit 75k. Take all trips away I have over 600k miles. Played correctly that's like \$80-100k in value. I actually was able to get the person who stole my miles name and personal information. I tried to add them on IG and LinkedIn (was not successful). Wonder if it's the same person
#10121	23-Jul-25	Reddit	mpones	20,000	I had 20k stolen a month ago. Called Alaska took 5 minutes they were back. Just my experience.
#10122	23-Jul-25	Reddit	luckynug		I had someone steal my miles and book flights with the same name is me. Alaska hit me with the same thing. They gave me control of my account had me set up a pin and I now have to call in if I want to use miles.
#10123	25-Jul-25	Reddit	Hot-Fig-4242	1,000,000	Just happened to me...almost 1 million miles I have been saving. Tickets were in the name of 3 Chinese people. They were flying Hong Kong to Doha to Toronto...business class on my miles. Glad I caught it before their flight in 3 days. Had to do the pin thing which sucks!!!! Keep in mind the hackers had to have your email or your airline frequent flyer number and your password. Sounds like an inside job to me or Alaska got hacked.
#10124	25-Jul-25	Reddit	being_bryan		Just found out today that my all my miles were stolen as well. Customer service is a joke. Al run around. This is ridiculous...

Ref #	Date	Platform	Username	Miles Stolen	Comment
#10125	25-Jul-25	YouTube	centsorsense	285,000	my Alaska Air account might have been hacked or there's some like super suspicious activity going on... I went on my phone to pull up my Miles account... like almost 300000 points gone... I'm like dude what the... like my points are just gone... they booked three separate 95000-point flights... I did not book any of these... so yeah this is like a massive fraud situation... I called Alaska... told them these were not my bookings they were like okay this is definitely fraud.
#10126	26-Jul-25	Reddit	Anxious-Astronomer68		I went into my Alaska app today to preorder food for an upcoming trip only to find that I had been logged out of my account. When I went to reset my password it told me that my email address was not recognized. I was able to reset my password using my mileage plan name and bday only to find someone had hacked my account changed the email and password and had booked themselves a flight using my miles from Newark to LA next week. I cancelled the fraudulent flight updated all of my passwords and reached out to customer care to see if I can add a pin or other 2 factor authentication. Looks like I'm not the only one either. This was reported earlier this week. My existing flights were paid with cash vs miles so I have to imagine that's the only reason the hackers didn't cancel them to free up more miles.
#10127	26-Jul-25	Reddit	Ok_Sir_7220		Happened to me a year ago. I now use a PIN each time I was never notified my information was changed. I just happened to be checking for an upcoming international trip and saw someone booked all my miles on 2 flights. Luckily I got it back.
#10128	27-Jul-25	Reddit	arolfe1980		Just checked and I'm missing a lot as well guess I'm dealing with this for the rest of my weekend
#10129	29-Jul-25	Reddit	TryLearnGrow	190,000	I just noticed someone stealing 190K miles from my account. I called Alaska and they cancelled the flight but I still have to deal with their mileage plan team to request to get these reinstated. A simple 2FA code during redemption would be so much easier to implement! I really hope they implement MFA for login and redemption process rather than keeping our miles behind this inconvenient PIN process.
#10130	30-Jul-25	Reddit	mikefly562	30,000	I had 30000 miles that may have been hacked and the wait time on the phone are very long. I'll most likely just never fly alaska again. Their systems are obviously not secure.
#10131	30-Jul-25	Reddit	Glass-Bobcat4357		Vent on customer service. Logged into my account this morning to see it was hacked. Used the chat bot and reset the password and updated my info. When I logged on saw all my points were drained. Chat couldn't help me so transferred me to someone else. Waited 30 minutes and said they couldn't help and to call the 1800 number. Called the 1800 number - requested a callback which they said estimated time was 25 minutes. Hours later nothing. So I call again. Been on hold for more than an hour. I would be freaking out less if I wasn't hacked and just needed some info. Frustrating.
#10133	31-Jul-25	KIRO 7 News	MC	150,000	Matt Cottingham found out months after his account had been broken into. He went to buy a flight and found it had been locked. After hours on customer service holds he says Alaska Airlines told him his miles had been stolen though they were refunded. The most frustrating part was they told me if it happens again there's a chance I won't get refunded and I'm like 'Well how am I supposed to know if this happens? How do you guys inform your customers?' The representative didn't have an answer for him. That was one of several questions KIRO 7 sent to Alaska Airlines regarding these apparent hacks. None of the calls and emails were answered. In Cottingham's case his 150000 miles was worth around \$1950 according to a NerdWallet estimate.
#10132	31-Jul-25	Reddit	bill_buttlicker1926		Same thing happened to me on the same day. Trying to call now to get them reinstated
#10134	01-Aug-25	Facebook	EF	430,000	Well I just got hacked on Alaska. Someone took 430k miles from my account and booked two tickets on Qatar airways. Alaska notified me and I'm on hold right now. There are no trips booked in my account but I added MFA on my account a while back when I heard about this. Has anyone been successful in getting their miles back? I don't know if the flights were flown or not because I can't see it in my account but it just happened a few hours ago and we are traveling overseas so I wasn't checking my notifications.
#10135	01-Aug-25	Facebook	LJ		mine was for what appeared to be a respected researcher at a university in NYC for a JFK-HKG flight. I definitely considered contacting the person it appeared to be directly to let them know that whatever site / agent they were using is a thief or at least uses questionable / thieving sources. After learning that some of the shady third party agencies on GF sometimes give people award bookings I decided not to freak them out by 'accusing' them of participating in fraud. Now I'm stuck calling in for every award booking because AS hasn't managed to figure out MFA in 2025
#10136	01-Aug-25	Facebook	MS		Sorry this happened to you it's happened to me and many others too and AS is great about reinstating miles. But they famously do not have 2FA/MFA maybe you're thinking of a different account? They're going to make you put a PIN number on your account to make redemptions it stinks.
#10137	01-Aug-25	Facebook	KAV		It happened to my husband on many loyalty reward programs and it took a lot of time and work but he eventually got them all back. Multiple credit cards we're hacked too as well as his fb and instagram accounts. Such a nightmare!
#10138	01-Aug-25	Facebook	TJ		Happened to me as well - even with a random computer generated 15 digit alpha numeric with symbols password. I feel like there's an exploitation in their website or rogue employee(s) selling info as it's highly unlikely anyone knew my password or personal information to book flights with my points. I didn't receive any emails of the points being debited or the flights being created - it's all pretty suspect in my opinion. The good news is that the points were reinstated in just a few days the bad news is that I have to call Alaska to book with my pin in the future. Good luck sorry that happened to you.
#10139	01-Aug-25	Reddit	netopiex		When my Alaska account was hacked they called in over the phone got them to change the email address and then reset the password. I had a long complex and random password it didn't help and it's not clear even 2FA would have depending how easily manipulable the CSRs are.
#10140	01-Aug-25	Reddit	sweetniblets	70,000	Mine was hacked as well (latter half of June). No email notifications to my legacy account email that the account email and phone number were changed two tickets redeemed at 35k miles for two different names just found out today. I did receive a whoole bunch of spam emails around that time and wonder if the hackers were trying to cover up any potential email notifications from Alaska that would've notified me of the account changes. I searched through my emails and didn't seem to get anything though which seems like a security failure on Alaska's side. Waiting on the refund of my points now after talking to CS. Added that pin to my account too...seems better than nothing.

Ref #	Date	Platform	Username	Miles Stolen	Comment
#10141	01-Aug-25	Reddit	lighteningbeam		I had my points drained recently too. Felt kinda sucky. They did put it back but now I have to phone in to use them ever - hopefully they have 2fa support someday soon. Looks like it's quite widespread saw a bunch of other similar posts
#10142	01-Aug-25	Reddit	olmsted	300,000	Yeah I had 300k+ miles plus some wallet funds drained from my account for flights from Lagos to Cairo (and additional fraudulent charges on a linked CC!). I am glad I check the app very frequently. I was able to cancel the thieves' tickets and get everything back without Alaska stepping in but I still notified them of the problem. They suggested that I let them lock my account which would require me to call them every time I wanted to book award travel. The idea of waiting on hold to use my miles because they couldn't be bothered with 2FA was not appealing to me so I told them I'd just go with a very secure password. They warned me that they would not assist me again in recovering stolen miles if my information is somehow stolen again (which... they didn't help me in the first place! I got everything back myself. If anything me supplying the data point was helping them). Really my only souring experience with AS (aside from BoFA fuckery on the CC side of things).
#10143	01-Aug-25	Reddit	joeychestnutsrectum		All mine were taken in June and they made it a pain to get them back and blamed me for it. Repeatedly told me that they wouldn't give them back again.
#10144	03-Aug-25	Reddit	Yuhreka		Chiming in to say the same thing just happened to me this morning. Someone had booked a flight to Hawaii using my Alaskan Airline miles. I only checked my Alaska Airline app because I got a Tript notification that my trip had been successfully imported. Turns out another flight was booked using my Alaskan miles few weeks ago. I didn't get any notice for that flight. And for some reason that mileage transaction doesn't even show up under my Mileage Activity in Alaskan Air app. I'm also one of the ones who recently transferred a bunch of my AmEx miles to Alaskan Air. Can I ask which number you called to report the stolen miles? I trying to call Customer Care and it's 2.5 hr wait. I also tried resetting my password and got a message saying something went wrong. didn't know about the grounding either. I've been on hold for about an hour. So I noticed that whoever used my miles to book the flight bought a ticket for me too. I'm guessing they were hoping to get an empty middle seat. I'm so tempted to just show up and sit next to them.
#10145	05-Aug-25	Reddit	urTypical20something	30,000	wait so how did you guys go about getting them back? had over 30000 miles stolen
#10146	05-Aug-25	Twitter	JMat2527		my account has been hacked twice in the past 4 months and I found out about the most recent one that happened a month ago. I am trying to contact customer care and I am on hold for past 2+ hours. Is there anyone who can help me asap recover my money.
#10147	05-Aug-25	US Card Forum	bibibibi	260,000	One morning my Gmail account was hacked and I received a large number of spam subscription emails (around 400+ in three hours). So I locked all my credit cards and started changing passwords for various accounts. A few days later when I logged into my AS account I found I had minus 260000 miles. On the day of the hack a ticket for ATQ-YYZ had been booked and had already flown away. When I checked my Gmail I found that an Alaska Revenue Protection email had been buried in my spam folder. Please call Customer Care at 1-800-654-5669 to verify your Mileage Account. There has been recent activity from your account that we suspect may have been done without your permission. Calling customer service they readily refunded my miles. The downside is that after adding a PIN to my account I have to call customer service and use the PIN to redeem tickets when trying to claim them. Another rant about AS's terrible IT - can't they just make a phone call when there's fraudulent activity.
#10148	06-Aug-25	LinkedIn	AB	185,000	Someone stole 185K miles from my Alaska Mileage account. I happen to log in to my Alaska Mileage Account and noticed a sharp decline in my available miles. Turns out someone just today redeemed 185K miles from my account for biz class tickets: Doha to London. It wasn't me. No idea how they were able to do this and neither does Alaska. But big shout to Alaska Airlines customer service team! They were able to credit back the miles within 40 mins. Going forward I do have to call their customer service and give a pin to book award tickets but it's worth it for the peace of my mind. PSA: to my friends and network please check your loyalty program mileage balance. Fraudsters are going after them. Alaska told me this is happening quite a bit recently. Stay vigilant!
#10149	06-Aug-25	LinkedIn	BEH		This same thing happened to me several months ago. Called and told Alaska Airlines what happened they credited back my miles opened an investigation and were fantastic the whole way. Their customer service is fantastic and why they are my favorite airline. I just wish they'd have more routes from DFW.
#10150	06-Aug-25	LinkedIn	CP		Someone did this and actually took one-way flight immediately with my miles. Pretty shocking since Alaska should have the identity of the person?
#10151	06-Aug-25	LinkedIn	CH		This happened to me last year same resolution. I'm unhappy that they will not increase account security through a 2FA which may not have eliminated the possibility of this happening but would have sharply reduced the likelihood of it occurring.
#10152	06-Aug-25	LinkedIn	DD		Same thing happened to me a few months back. Got them back but wasn't fun!
#10153	06-Aug-25	LinkedIn	DBC		This happened to me a few months ago lame to have to call in with a pin number but it's worth it to not have this happen again. Yours is almost identical to mine.
#10154	06-Aug-25	LinkedIn	JW		I had this happen not long ago. Took forever to get fixed and they acted like it was no big deal. I was not happy.
#10155	06-Aug-25	LinkedIn	JEW		Exact same thing happened to me. Team was great helping. Curious it's happening frequently. Strangely it was Qatar Airways flights as well.
#10156	06-Aug-25	LinkedIn	KM		Happened to me. The call in seems like a pain but Alaska Customer Service makes it easy and its handled within a minute or two.
#10157	06-Aug-25	LinkedIn	LW		Same thing happened to my daughter a few months ago but Alaska customer service resolved it quickly
#10158	06-Aug-25	LinkedIn	TC		This just happened to me too!
#10159	06-Aug-25	LinkedIn	VD		Same happened a few months back. Fast resolution from Alaska team but worrisome it keeps happening. Check email for 'Alaska Airlines Vacations powered by Expedia'—appears to be where breaches occurring.
#10160	07-Aug-25	US Card Forum	w8803809		This morning I experienced the same thing as the original poster: first a bunch of sub-emails then I logged into AS and found two business class accounts with Chinese names in my account...
#10161	10-Aug-25	US Card Forum	ait		I also encountered the same problem as the original poster today. I'd like to ask if you contacted AS after you canceled? My email address wasn't changed I just canceled the other party's flight and changed my password.

Ref #	Date	Platform	Username	Miles Stolen	Comment
#10162	18-Aug-25	Twitter	NoahKline	250,000	Hey AlaskaAir my mom's 250k miles were stolen. She's a retired nurse who saved for years to visit her grandkids in retirement. Customer service says they can't help—but your breach shouldn't punish loyal customers. Please make this right
#10163	20-Aug-25	US Card Forum	koalajiang	190,000	August was a month of bad luck my P2Case account was banned. Today I received an email about my Alaska Atom card application and noticed my mileage had decreased. I logged in and saw that I had selected reward activity. On August 12th an Indian customer bought a QR HYD-ATL business class ticket (190k miles). Strangely I didn't receive any confirmation email. I guess they chose not to send me an email at checkout and paid the taxes with their own card. I called customer service uploaded my driver's license and set up a PIN number. From now on I must call to unlock my account before buying tickets otherwise Alaska won't help me if I encounter fraudulent transactions again.
#10164	21-Aug-25	Reddit	coconut723		This just happened to me. WTF!
#10171	25-Aug-25	TikTok	chynawithawhy		Needless to say I was on the phone for another 2 hours after I realized my miles were GONE 😭 #fyp #foryou #alaskaairlines. Hacked Alaska Airlines Account: Lost Miles Recovery. Discover how to recover lost miles after a hacking incident on your Alaska Airlines account. Protect your travel rewards today! #alaskaairlines #milesloss
#10165	25-Aug-25	US Card Forum	Scotch	100,000	Holy crap my account got hacked too! My email address was completely changed without my knowledge. Last time I couldn't log in I just gave up and didn't bother logging in again. Today I wanted to change my password and then I found my email address had been changed. Sigh I guess I'll have to play again tomorrow. I've been seeing Tan You's AS account get hacked every day and now it's finally my turn. Did you manage to recover all your miles? Luckily I didn't transfer them from MR to AS last time but there's still almost 100k miles left...
#10166	25-Aug-25	US Card Forum	yun520cn		I just applied for a Summit card and my account was hacked and I received a mileage ticket. I don't know if it's a coincidence. Mine too. Delete the email address used to hack my account then change the password. Looks like quite a few things were stolen.
#10167	25-Aug-25	US Card Forum	divinebaboon		Yes a friend of mine was hacked last week.
#10168	25-Aug-25	US Card Forum	Cai Xukun in the US		My account got hacked and nobody uses my points.
#10169	25-Aug-25	US Card Forum	It's cold.		A few weeks ago someone also booked a hotel for me but luckily I found out early.
#10170	25-Aug-25	US Card Forum	dajidan		Yes about two weeks ago I had the same symptoms and my account was hacked. The authorized customer service representative wasn't working on weekends. Why can't you just add a 2FA to AS?
#10172	27-Aug-25	US Card Forum	Sandglass9		When I finally wanted to exchange it I couldn't by the time I got to business hours the tickets were all gone.
#10173	01-Sep-25	Facebook	VA		can confirm that sometimes alaska for JAL is not phantom. Unfortunately my alaskan miles were stolen so now I have to call in to get any award bookings and by the time I was able to do that the flights were all gone. Had gotten through to checkout on alaska before it directed me to call in.
#10174	01-Sep-25	US Card Forum	lty900301		I just logged in and discovered my account was also fraudulently charged on July 15th. Can I get a refund by contacting customer service?
#10175	01-Sep-25	US Card Forum	lijing		My account was hacked right after I applied for the card. Could there be an inside job waiting to complete the sign-up quota and then steal miles? I have 30000 miles in my account but the hacker hasn't issued any tickets yet.
#10176	01-Sep-25	US Card Forum	ygsq		To all the students upstairs whose PINs were stolen is anyone else fed up with waiting an hour to unlock their PIN and missing their tickets and deciding to cancel their PIN? And having to call again every time there's a change... I really can't take it anymore... Don't you know how to use a complex password generated by Apple to change your contact email to a more complex one? Or you could transfer the points to HA and then transfer them back when you need them. What do you all think?
#10177	02-Sep-25	Reddit	Remote_Lobster5345		this just happened to me. Crook changed the email address and I was never notified of the change. I found out something was off when i couldn't get into my acct and a password reset was sent to an email I didn't recognize. I called Alaska and turns out my miles were redeemed for flights that were flown already. I got the miles back but now need a PIN to redeem in the future. It's crazy that they don't have 2FA and don't send an alert that my email was changed. I have the names of the people that flew and the email address that it was changed to. Not sure if there's anything that can be done there esp. if Alaska is not going to do anything since they have the same info.
#10178	04-Sep-25	Twitter	fananator	300,000	My AlaskaAir mileage account was hacked and over 300k miles stolen. Customer service was informed 8/6/25 and promised to make it right. Since then no response. No response to email . When I called again no further help! What can I do? thepointsguy OneMileatATime
#10179	04-Sep-25	Twitter	insaneakash		Hi AlaskaAir my miles were stolen and after a 2+ hr wait I finally connected with customer care who helped restore my account and told my miles would be back. It's been over a week since then but I've received no update on when my miles will be returned. Can you please help?
#10180	08-Sep-25	Reddit	achinda99		This happened to me recently and after following up with Alaska I was able to get the transactions reversed and points readded. They did give me some shade for not having a PIN on the miles account but I never recall that being an option/suggestion. Now atleast the PIN prevents unauthorized transfers. That said what was weird was that my account was hacked email changed. So I couldn't access my account either during this time. According to them 2FA is coming soon.
#10181	08-Sep-25	Reddit	GoatRenterGuy		Miles Stolen. No 2FA? Just booked a flight with Alaska and noticed I don't have any miles. Looked at miles activity and saw two Expedia transactions that I did not make they had updated primary phone number and email address. No notification about this at all. No way to enable 2fa on my account. It is 2025 and there isn't 2FA on account that can be worth thousands? Still on hold trying to get my miles back. This is extremely disappointing. Alaska has lost my trust.
#10182	08-Sep-25	Reddit	drewbinator	60,000	This has happened to me. I lost 60k miles. The worst part is they make you put a pin on your account YOU HAVE TO CALL TO REMOVE. You sit on hold for hours just to use miles. You won't be able to book with miles outside of business hours.
#10183	08-Sep-25	Reddit	SnuSnuCupcakes6969		Call customer service and ask for Revenue Protection its a department that helped take care of my stolen miles. They actually emailed me when my miles all disappeared over a couple weeks saying that they thought it was suspicious. They put a pin on my account for me and recovered my miles.

Ref #	Date	Platform	Username	Miles Stolen	Comment
#10184	09-Sep-25	Reddit	thetork7		Happened to me recently. I got an email spam attack and knew something fishy was going on. I checked all of my bank/credit/mileage accounts and noticed a ton of Alaska miles were gone. Two people treating themselves to Qatar Q-Suites tickets. Thankfully Alaska was able to cancel the res before the tickets could be used. I noticed it over the weekend and had to wait until Monday morning to get it resolved which was irritating. All miles were reinstated.
#10185	09-Sep-25	Reddit	2000subaru		If you call them and explain the missing miles they will add 2FA to your account as a precaution. Happened to my wife but I do t understand why it isn't on every account.
#10186	11-Sep-25	Reddit	Low_Somewhere_978	30,000	beware of fraud from possible Atmos Rewards website. I just wanted to share that I just experienced fraud on my account. Someone hacked into my account changed the email address and then booked two award tickets and used 30000 points to book these fraudulent tickets. I only noticed because I got a notification on my app and I was still logged in and the trip showed up under my trips and then I panicked! So one of the agents told me that ever since they launched the new Atmos rewards program they have been seeing a lot of fraud. I changed all my passwords and had to verify my identity with the fraud department and everything got straightened out (the tickets were canceled and I got my points back thank goodness) but then I went to log into the rewards account and sign in with my new password using Safari and the warning came up that said This Connection Is Not Private This website may be impersonating www.atmosrewards.com to steal your personal or financial information. You should go back to the previous page. This never showed up when I accessed the site on my iPhone OR on Google Chrome!!! I also downloaded the new Atmos Rewards app so now I'm scared it will happen again. I'm deleting it. I highly suggest everyone stop using that until they fix their security issues. same they told me that I would have to contact them if I want to book an award ticket too but maybe when 2FA comes into play they will change that. They told me it won't happen until the integration is complete with Hawaiian mileage plan which I think is October 1.
#10187	16-Sep-25	FlyerTalk	ghina	123,000	Rewards number removed from acct and 2 flights booked So it looks like my account has been compromised. I'm on hold with Alaska. Awardwallet notified me that I had just lost 123K points. When I logged into Alaska I was told that an Atmos Rewards number is needed. Please call Guest Care at 1-800-654-5669 to add an Atmos Rewards number to your account before you continue. So that was stripped from my account but points were redeemed as well but not all of the points just enough for a nice Intl flight from JFK to KIX twice. Apparently this happened a week ago. I'm just putting a data point out there it could be a glitch it could be malicious but you may want to check your accounts. No explanation but they've credited the points and locked my account so now I have to call to book and provide a pin.
#10188	18-Sep-25	Twitter	spikeoren		1.5 hour wait time to get through to an agent when my Atmos account has been hacked and been used fraudulently is simply not cutting it. Please reach out directly
#10190	18-Sep-25	Twitter	a_pathak5		My account was hacked points redeemed and a ticket purchased. Need urgent assistance.
#10191	20-Sep-25	Reddit	Itchy-Guava		Can confirm - I canceled someone else's flight on my account then locked my account for miles redemption. I had to email them my ID.
#10192	20-Sep-25	Reddit	westbysw	250,000	I had it happen with 250k miles and contacted them immediately. The person didn't fly in my case. Obviously changed my password and they redeposited but I put a pin on using my miles until they do the two step verification so it's only unlocked by me calling which sucks but prevents it from happening.
#10193	20-Sep-25	Reddit	wynag	25,000	Logged into my Alaska account to check on another flight and 25000 miles have been stolen from my account and moved to another completely random guys account to book a flight. It shows his name and flight on my account and allows me to cancel / change the flight. Flights on Tuesday. Obviously going to call Alaska in the morning to figure out how I get these points back and what I do but has anyone had this happen? Any advice would be greatly appreciated. Also - How does Alaska not have two step verification as an option for accounts?? Are we in 2010??
#10194	21-Sep-25	Reddit	DueString2621		Alaska forced me to put a pin on my account to get the miles back (even though they used my points to sell a ticket to a random person with a bogus credit card). I got the miles back but then when I tried to use them I had to call and was on the phone for almost 2 hours until someone could unlock my account. I told them to keep it unlocked since I didn't care if the points were stolen again because I'm NEVER flying Alaska again. I switched this year from delta since I've heard status/upgrades are easier but not worth it between always being delayed and this situation.
#10195	21-Sep-25	Reddit	Greensky_613		Happened to me too. I called customer service they stopped the guys at the gate. Refunded miles. And put a pin on my account
#10196	23-Sep-25	Reddit	Finebonechina1		Not sure if this is relevant...I made two bookings (hotels) with Alaska points in the summer and still had a points balance. No warning whatsoever...logged in to day to find this is now administered under Atmo. There is no detail on my bookings and it says I have no balance....after 12 years of paying in to this program!!! Seems like someone in the corporation has found a way to take my pints and leave me hanging. Very dirty play on the part of the reward program administrator. Anyone else found similar?
#10197	25-Sep-25	FlyerTalk	FragranceMarketingGuy	215,000	Hacked As Well Looked at my Points Activity and noticed 2 Qatar 215000 tickets deducted. immediately called Customer Care and have to follow the Pin Restriction until Dual Authentication arrives (supposedly in a few weeks). Points immediately redeposited after I sent in my ID.
#10198	25-Sep-25	FlyerTalk	sbedelman		This is same experience I had. It was a hack. Multiple tickets issued for travelers originating in China. The first thing they did was change the email address on the account (no flag of this by Alaska) so the reservation confirmations went to them. I immediately called the airline. As with you the reservations remained on my account but clicking through gave the same error message and my miles were reinstated so what we experienced appears to be the standard procedure. It was just luck that I signed into my account that day.
#10199	28-Sep-25	Reddit	Margaritasinthesun	350,000	350000 miles stolen!!!! On Sept 9th 350000 miles were stolen out of my account. Two tickets flown SFO-TPE with the flyers names on them showing in my app. Email on the account was changed. Called customer service who requested my license via email. Waiting on response. Outrageous that I never received an email notification that my email was changed nor is there a 2fa option on the account. How long do I have to wait to get my miles back??? Are they going to do anything to the people who flew the ticket??? Just got off the phone with AS rep after waiting 2 hours for a callback! All the miles were returned to my account today with the caveat that the account is on permanent lock unless I call in with my pin to book. I'll take what I can get at this point.

Ref #	Date	Platform	Username	Miles Stolen	Comment
#10200	28-Sep-25	Reddit	cowlton		I had this happen with alot less points though. They booked a flight same day but I was able to cancel it before flight. Alaska replaced miles no problem and put a lock of my miles with a pin which is a real pain in the ass because I wanted to use them recently and had to wait for rewards to open the next day and my flight increased quite a bit. How they dont have 2 factor authentication is beyond me
#10201	29-Sep-25	Reddit	07traybay	75,000	Same thing happen to me ! I was able up cancel the ticket. I had my 75 miles returning.
#10202	29-Sep-25	Reddit	Difficult_Rhubarb174	70,000	This happened to me a few months ago. They will get the miles back to you. Mine came back in a few days. I'd bet you didn't get an email because they also changed your primary email to theirs. You now get to join the fun club where you have to call to get your miles unlocked so you can use them. I'd rather be slightly inconvenienced and not lose 70000 miles again.
#10203	29-Sep-25	Reddit	SyntaxError_22		Same thing happened to my friend recently and she worked with Alaska Airlines to get the miles back.
#10204	29-Sep-25	Reddit	wannabebondgirl007		They'll fix it and I got my miles back immediately but unfortunately it comes with a forever headache. Your account will be forever locked. Whenever you want to book mileage you'll have to call and unlock your account. Of course it's great to be protected but the customer care office is not open every day and closes at a certain time. Whenever I tend to have a chance to sit down and look at reward travel it tends to be at night after work which is when they're closed.it's been a year now since my account was compromised
#10205	29-Sep-25	Twitter	PR	750,000	I had Hawaiins mileage acct for a very long time no issues. Since 'Atmos' came along I have been hacked twice for 750 thousand miles now to use my points I have to call in (not on Sunday) they will unlock my acct for one hour so I can book flights then they lock it again. I am not the only one. Be wamed Alaska Mileage is ripe for hacking. Watch for flights booked on Qatar and Japan Airlines for international travel. Read about this and check your Atmos account DAILY! YOU HAVE BEEN WARNED.
#10206	30-Sep-25	Reddit	spazmboy673	370,000	I just had 370000 of my alaska airline miles get redeemed. Im currently on hold right now for a rep... reading your post gave me hope because i have been stressing out for over an hour.
#10207	30-Sep-25	Reddit	Jwfrir		I had the same thing happen to me but before the flights were flown. I was also freaking out but managed to get the miles back. Alaska's fraud detection system is WOEFULLY terrible. Someone booked a flight between 2 cities I'd never flown in F that I never fly with a name I've never used using all of my miles on a partner airline. Each of those individually should trigger a 2 factor authentication or fraud screen. It's insane they let that get booked. I don't know if them having flown the flight it'll be as easy for you. Hopefully you'll get them back They also added a pin for any future use of miles
#10208	30-Sep-25	Reddit	Loving-my-Pyr	50,000	Yes you will get them back. Three years ago I had 50K stolen and the thief used my airlines credit card too. Everything was refunded in less than 24 hours. Now I get a text every time my CC is used. And there is a block on my acct to use miles. I have to call them and they unblock it for one hour. This works VERY WELL.
#10209	03-Oct-25	Twitter	cardopdx		my account has gotten hacked 2x within a month! Twice I have checked my account and a random flight has been booked for the thief! Please fix this! Yes I changed my password when you guys first tried to resolve this and added a pin. Howwww does this keep happening?!
#10210	11-Oct-25	Reddit	zoenberger		Was your account hacked? Happened to me. The person got in changed my email and phone number and then bought a ticket. I couldn't login and when I tried to reset the password on the web I'm assuming the reset emails were going to the other email on the account. I got lucky and the mobile app still had an active login session so I was able to figure out what was going on. I changed my email back and reset the password. Better call Alaska and find out if miles are missing also.
#10211	13-Oct-25	Reddit	PNWPlayZ	95,000	I had my account hacked for about 95k miles. Reimbursed but was a big headache
#10212	15-Oct-25	Reddit	dank414	65,000	It just happened to me... I just noticed several flights were booked by four people flying to Miami and Las Vegas.. They flew in August and October. They burned 65000 miles. I hope I can get this back. I didn't get a single email confirmation that it was used.
#10213	16-Oct-25	Twitter	goisles94	55,000	y account gets hacked and 55k miles are stolen. I am given two options: 1. Call EVERY SINGLE TIME I need to use my points OR 2. Book online but if miles are stolen AlaskaAir WON'T recover those points.. AlaskaAir How does that make sense?! Need explanation!
#10214	18-Oct-25	Twitter	jovoych	304,000	had 304000 point stolen from my account in February. Someone changed the email address. What can I do I worked hard for that
#10215	27-Oct-25	Reddit	Calm-Refrigerator910	50,000	This happened to me this AM! Got an email Sunday that someone redeemed 50k miles. I contacted them via chat and they said closed on Sundays call Monday. I did at 7 AM PST right when the open and thank god I did because the fight was for this morning. She said they cancelled the ticket and put a no go status on it if they show up and try and fly. At least they sent the email otherwise I would have never known! The crazy thing is to unlock my account now they want me to email a copy of my drivers license. I had to educate them that this is EXACTLY why fraud is so rampant what if they have my email password (now or at any point in the future) and now the scammer has a copy of my Drivers license? I don't think so. You'd think these mega companies would have a way or you to upload or send securely?
#10216	29-Oct-25	Reddit	chuchifrito	130,000	Alaska/Atmos Security Breach! Had 130000 rewards points stolen through a booking made on Alaska Air website for a ticket by a foreign airline Starlux from LAX - HKG. Impossible to get an answer or assistance from Alaska/Atmos. Best thing I've gotten is an auto reply from customer service saying they will get back to me in 3 weeks... Been an Alaska card member for over 10 years... No loyalty and no service.
#10217	29-Oct-25	Reddit	Curious_Gas_2608		Need to call them (Alaska) back ASAP. They are able to cancel that ticket and refund the miles - but very important to do it before the scammer flies. This happened to me a couple years ago and they took care of it all over the phone. If the first rep can't help you ask to speak to a supervisor.
#10218	29-Oct-25	Reddit	mtcizzle		My friend had the same thing happen last week. She called CS they refunded her miles and now she needs to call CS to authenticate before any purchase with her miles. They told her 2FA is on its way! Agreed not AS's fault (she had a weak ass password she reused that was part of a breach on another site) but nice to see they took care of her.
#10219	29-Oct-25	Reddit	seahawks101777		This happened to me last year I called and they were super helpful. Got me my miles back and I had to call in every time I wanted to use my miles for a bit. So no I wouldn't say calling in is useless OP. Sorry you didn't get the answer you wanted.

Ref #	Date	Platform	Username	Miles Stolen	Comment
#10220	29-Oct-25	Reddit	blazerlazer18		Police report won't do anything. Contact Alaska and get your miles back or money and then they will lock your account so if someone gets access to it they won't be able to use the miles. It is because the lack of 2 factor authentication that it is easy for people to get into accounts. Happened to me before.
#10221	30-Oct-25	Reddit	ivorytowerescapee	100,000	This has happened to me too - about 100k miles stolen and used to book an adult only resort in Spain. The main Alaska line said the only way was to let it go and they'd refund the miles just this once but their hotels customer service cancelled the reservation. I spent at least an hour+ on the phone I was pissed. My password is very strong now.
#10222	30-Oct-25	Reddit	Prize_Emergency_5074		Shouldn't be so easy to change key info on accounts like. They changed my phone # and email address with the same ease as I did changing them back. Somehow I was still able to access my account thru the app and make the changes. Big holes in security here. Just got off the phone with CS and said the same. The solution is to add a PIN code to my account which would require me to call in anytime I wanted to access the site. I said no thanks I'll take my chances with my new password rather than have to go through all that. Yeah screw that pin bs. That's too much work just to access your account. I hope everything got straightened out for you. Took 2 1/2hrs but AR made things right.
#10223	30-Oct-25	Reddit	Away_Association_636		Yep same thing happened to me a week ago. I just randomly check my account sometimes to make sure my credit card points/miles are transferring over. Just so happened to check it late Thursday night and found three tickets were purchased with my points and were scheduled to leave an hour later from Dubai! I was fortunately able to cancel the tickets in time and got my points back. They had changed my email too but left my phone number and I had not received any texts or push notifications about this flight which normally I do. Changed the email address back to my own changed my password and contacted Alaska. Was told the only thing they could do for me is to lock my account and I'd have to call and use a PIN anytime I wanted to book a flight using my points.
#10224	30-Oct-25	Reddit	Amazing_Scallion9548		My account got hacked. Just giving a warning someone hacked into my account changed the email associated with my frequent flyer number to itsallthere404yahoo.com and flew with my points. Currently working with Alaska for them. to reimburse my points. But it's a long process and going forward I can't use my points online to buy. Sounds like this happened before when I was talking to the rep
#10225	31-Oct-25	Reddit	gwshark101	175,000	This happened to me last month. Someone named Longcheng Zhang took all 175k points in my account and bought a starlux flight JX LAX-TPE. Got it refunded and now I'll always have to call AK to unlock my account whenever I want to book a flight.
#10227	31-Oct-25	Reddit	Bostom		Same here. Their system is terrible since it makes it out like it's your fault.
#10226	31-Oct-25	Twitter	misskatmaster		AlaskaAir why is it now my problem because you have had a security breach? Two 2 hour phone calls and nothing resolved. Stolen points and my flight cancelled by fraudsters! Shame on you alaskaair you take better care of fraudsters than your real customers!
#10228	01-Nov-25	Reddit	Capable_Phrase4900		Account hack - twice in one day even after changing password. Hacked atmos account TWICE in one day even after changing password. How does that even happen?? Couldn't get through to customer care it was a 3+ hour hold time. Tried again this evening when I found the second hack and another person flying on my miles...30 minutes and waiting. Both flights were still in the air when I found out but there is absolutely no recourse to flag it quickly to get the perpetrators at their destinations. The web chat agent said they couldn't help and to just wait in whatever length of queue there is. I've been loyal to Alaska for decades but this is really changing my mind
#10229	01-Nov-25	US Card Forum	ltty		Holy crap I just discovered my account was hacked. I just applied for Atoms and completed the sign-up requirements. My phone number and email address were completely changed without any warning. I only found out when I couldn't log in to book. I booked tickets for the next day and they flew yesterday. They issued seven tickets from PHX to SAN with seven Middle Eastern names all with the same last name. It's outrageous.
#10230	02-Nov-25	Reddit	CharChar7007		I've been reading through these discussions after staying up last night dealing with the same issue. It's unbelievable that Alaska still doesn't offer basic two-factor authentication — and even more concerning that they don't send email notifications when account contact information is changed. This isn't just about stolen miles or the countless hours many of us have spent trying to recover them. These accounts also contain highly sensitive personal data — in my case all my family's travel information including passport numbers Global Entry details and birthdates. It's unacceptable that such data isn't better protected. I'll be reaching out to Alaska today to let them know that unless they address these serious security gaps I won't be using their services in the future. This level of oversight is simply unacceptable in today's world.
#10231	02-Nov-25	Reddit	BeachView4		I woke up yesterday to an email from Alaska thanking me for redeeming points for flights. Overnight my account was hacked and three tickets were purchased. I immediately changed my password and called customer service. The flight booked was for later that day and I believe Alaska was able to cancel the reservations. I was told the points would be immediately put back into my account (hasn't happened yet). I was also told my account would be locked. An email would be sent requesting a picture of the front of my drivers license and at that point my account would be unlocked. I just received the email but they are also asking me to create and include a PIN for my account which I will need in the future to redeem points. I've never had a company ask me to email them a PIN which doesn't seem very secure. I have no problem emailing my DL but including a PIN seems weird. Has anyone else experienced this?
#10232	02-Nov-25	Reddit	Striking_Prune_557		This happened to us as well.
#10233	03-Nov-25	Facebook	PW		Someone hacked my mileage account. They gave me the option to wait 2 hours on hold or get a call back. This is so inconvenient
#10234	03-Nov-25	Reddit	Sweaty_Sea_524		Same thing happened to me and it's ridiculous because now we're being punished for our accounts getting hacked. Now we have to call during their business hours and be put on hold just to give them a pin and redeem our points.
#10235	04-Nov-25	Facebook	KMW		I had this happen and used the chat feature. The person used them for a ticket. I did get them all back.
#10236	04-Nov-25	Reddit	jeongminjeon	125,000	Mileage points stolen and I cannot talk to customer service. Holding time is more than an hour.
#10237	04-Nov-25	Reddit	WorkingFederal6746		Called Customer Care and recording said wait time was ~2 hrs left callback number. Agent called back and resolved problem.
#10238	04-Nov-25	Reddit	DamnEngineer1960		Yep. Happened to me a couple years ago. Someone from China bought tickets to LAX. Luckily the flight was in the future and Alaska cancelled it and restored my miles. And I still have a PIN

Ref #	Date	Platform	Username	Miles Stolen	Comment
#10239	04-Nov-25	Reddit	Brilliant-Camel-1600		I was hacked 2 days ago. Spent 5 hours waiting for customer care to pick up the phone. The hold assist function with the new IOS 26 made the process a little more bearable
#10240	04-Nov-25	Reddit	oleniko		Had this happen you'll get it reversed. Be patient.
#10241	04-Nov-25	Reddit	tfthisallabout		When this happened to me I also got signed up for 1000s of emails - did this happen to anyone else? I did get my points back and Alaska cancelled the flight that wasn't booked by me
#10242	05-Nov-25	OneMileAtATime	Breanna		Nice that it was easy in this situation. For us normal people it has taken over a week multiple calls and placements on hold several communications with several AKAir reps who ALL neglected to remove the fraudulent email from my account leaving me remaining in a locked out state multiple rude engagements with people who did not care to listen to the actual issue and stress and tears. Were the miles replaced eventually- yes. Did it compensate in ANY way for the treatment and endless circles endured. NO. This was truly one of the most unpleasant experiences I have had to deal with in a very long time and while the miles were returned I continued to be treated like "I" did something wrong- even through multiple representatives continued error. I was told you seem to have just gotten the short end of the stick and that is all I can say. "I" removed the fraudulent email from my account after 3.5 HOURS of going in circles today alone. What a joke.
#10243	05-Nov-25	Reddit	Flimsy_Letterhead596		Same thing happened to me a few months back and I went through the same process you described. I also thought asking for a PIN via email was weird but went along with it... I'm sure I'll regret that!
#10244	10-Nov-25	Reddit	0520BB	112,500	The exact same thing happened to me. Apparently on July 28th someone hacked my account. I know it's natural to assume I did something in some way to cause my account to be hacked but that's not the case. I only use my app when I need to book a flight or while I travel neither of which I had done since more than a month prior to that. I was not anywhere near my AA account in July or August. On 8/22 I got an email from Atmos explaining the switch and it said the login information is the same as whatever I used for Alaska Airlines. I tried to login and it said the password was incorrect. I tried to have the password reset and it told me an email was being sent to an email address (not fully shown just the first letter followed by a lot of asterisks and hotmail.com) that was not mine. I've only ever had the same gmail. I tried three times and it showed the wrong email each time. I honestly thought there was just an error on Atmos' end when they transferred our information into their system. cShe confirmed my account was hacked on 7/28 and that they took 112500 miles. Three flights were book on Starlux and the names are listed. They obviously changed the email address so I didn't receive confirmation emails about the miles being used. I asked how they changed my email address on 7/28 to steal miles but Atmos had my correct email on 8/22 when they sent the reminder email and she didn't have an answer. She made me give her my real email address then she sent me an email and asked me to email her back a picture of my driver's license and a four digit pin of my choosing. Apparently this restricts my account now and I will forever have to call and give my pin if I want to book flights with my miles. I told her that it was disappointing to know that because they didn't have any sort of multi step verification process in place that I would forever be inconvenienced to have to call to book flights now. I actually brought up my husband's account and asked if we should put his in restricted status and give him a pin if that was the only way to ensure no one could just easily hack his account change his information and steal his miles. I basically got her to say that Atmos accounts are NOT safe right now because there is no multi step verification process before changing personal information or to use the miles. She said she understood my frustration and put me on hold (as if 3+ hours wasn't already enough) to go speak with her supervisor. She came back and told me that they are going to be coming out with a 3 step authentication process very soon so there is no need to put the pin restrictions on my husband's account. She told me that emails will go out notifying us at that time and when that happens I won't have to use the pin any longer. In the meantime the customer service rep is supposed to be opening a claim to get me my miles back. No time line was given. I sent my driver's license and pin via email and never received a response. I sent a follow up email a few days later asking for verification of receipt. I reminded her that since I was already hacked and feeling vulnerable asking me to email private information like a driver's license via email and not in a more secure fashion was making me nervous and really highlighting their lack of security. I still haven't gotten a response or gotten my miles back. We'll see. It's crazy to ask customers to spend hours and hours of their time just trying to get support. Sounds like Atmos needs more employees better management and much higher security levels! It might be time for me to step away from Alaska Airlines.
#10245	16-Nov-25	Facebook	PJ		Hello! I just had someone fraudulently book a trip through my Atmos account using my points on Iberia last night. Horrified I cancelled the trip and changed my account password. This caused my points to be credited back to me thankfully. I would like to turn on MFA but I don't see that option. I chatted with reservations and let them know. Has anyone else had this happen? Is there anything else I need to do? I have 90000 points which obviously are with a lot of money. Thanks!
#10246	16-Nov-25	Facebook	MJM	83,000	I had it happen and was notified by Alaska last week. I went from 180K+ points to 97K. I had to submit a bunch of stuff to identify myself and was told unless I set a pin I will not be credited if it happens again. Now I will be required to call and unlock my account before I can book award travel. That will be a royal pain but I don't want to risk losing points again. I cannot change my password without calling. So the account is locked with the old password on it.
#10247	16-Nov-25	Facebook	CH		Same here. Yes I had this happen and it took a few weeks to get all of them back.
#10248	16-Nov-25	Facebook	TM		It happened to me too. Business class tickets to China. Luckily found it right after it happened. Immediately cancelled got points back and using Apple PW manager changed to theoretically uncrackable password. The problem with locking the account is that you have to call customer service and they aren't available 24/7. Allegedly working on 2FA.

Ref #	Date	Platform	Username	Miles Stolen	Comment
#10249	16-Nov-25	Facebook	JDF		Same thing happened to me in August. I only found it when I began an initial search for a spring trip to Honolulu. I noticed a huge amount of points missing. Then looked at my trips and found a trip taken throughout Colombia and another booked for the next day. I tried to cancel the flight but couldn't. The name phone number email and even the date of birth had been changed in my account. I very frustrated called customer service. After a 3 hour wait I received a call back. What a hassle. Anyway that next day's flight was canceled. I actually asked Alaska Air to have police meet the person at the airport but they wouldn't. Customer service gave me back all of the used miles. The biggest hassle was getting account access returned to me. That took about 3 days. I had to provide my drivers license as well as speak with a few Alaska Air team members to verify I was me. Thank goodness I didn't have my credit card number saved an only miles went missing. I have a pin on my account now and must call CS to book trips using mikes. I was very surprised such changes to my account could be made in the first place. Hackers are pretty savvy!
#10250	16-Nov-25	Facebook	HH	150,000	I had that happen too. They took 150000 points and booked a Tokyo-LAX flight. Fortunately I was able to call and get it cancelled and points returned. And I'm an employee.
#10251	16-Nov-25	Facebook	DE	310,000	it has happened to me several times. Unfortunately they'll make you freeze your account or they'll threaten to refuse to refund your points next time. I've had 310000 points removed even when it was supposedly frozen. So it's definitely a known problem and a big problem. I've definitely avoided booking with them for this reason.
#10252	16-Nov-25	Facebook	RBB		This happened to me. They had me create a PIN number that is used only when redeeming points
#10253	16-Nov-25	Facebook	NC		This happened to me. They eventually credited my points back. I have to now call in to have them unlock my account for a couple hours if I want to book trips using points. They don't have mfa unless that has changed. It's annoying to have to call in and have them unlock my account.
#10254	17-Nov-25	Facebook	CPB		I had this happen. My acct to use miles is now locked so I have to call them and they unlock it for an hour. It could be a pain. But not as painful as somebody stealing your miles.
#10255	17-Nov-25	Facebook	KO		I had the same thing in August. I looked up the confirmation and canceled the trip and got my miles back.
#10256	17-Nov-25	Facebook	HR		I only knew about this when I was booking a ticket for a friend. Alaska website asked if I want a confirmation to be sent to a different email. I put in her email. After the booking is done Alaska never notified me that my points have been deducted and a trip had been booked. All communication was sent to my friend's email. Typically the airlines will send an email to the account owner when miles are being deducted from the account but nothing is sent from Alaska.
#10189	26-Nov-25	Reddit	PharmerDale		It was particularly fun when you couldn't remove them from a drop down list of previous "companions." Booking a flight for my wife and I'd have to scroll past 3 African names before getting to my wife. At least AS figured out how to let us remove companions. Now I have to call in with a PIN any time I want to use miles or an upgrade cert.
#10257	26-Nov-25	Seattle Times	user1042510	100,000	I had 100K of my miles stolen from my Alaska account in summer of 2024 but Alaska immediately refunded them and implemented an extra security feature where I had to call customer service and provide a PIN number to unlock the ability to use my miles. I haven't had any issues since. This article doesn't mention the extra security Alaska put in place to protect my miles.
#10258	26-Nov-25	Seattle Times	user1112343	160,000	Three years ago 160000 miles were stolen from my Alaska Airline's mileage account. I noticed it about 2 hours before the flight was to depart Doha Qatar. I had the travelers name passport number etc. I called Alaska and alerted them but they would do nothing. I found the perp on instagram and saw pictures of him and his lady toasting their travels with champagne! Alaska did nothing but ask me to change my password and require that I call them to unlock my account whenever I want to use miles. The dept I have to call is only open 8-430 weekdays. So very inconvenient especially when traveling abroad. The login j used for Alaska is different than any login I use for anything else. They need to institute two-factor identification for login. It would solve the majority of these issues. I only got my miles back after I tagged @alaskaair on social media. They contacted me IMMEDIATELY after doing so.
#10260	27-Nov-25	Seattle Times	user1060599	150,000	Same story here. A couple of years ago I had 150K+ miles drained from my account. At the time a bad actor knowing only your Mileage Plan number could initiate a password change. The fraudster changed my password and the account email address then purchased flights for themselves. Alaska's 1990's-style IT security did not alert me to any of this I only found out when trying to log into my account weeks later. Virtually every other type of online account will sent an alert to the current email on file if basic account information is changed. And of course 2MFA has been around forever. But Alaska prefers to force its customers to lock down their account with a PIN only usable during certain hours when you need to book with miles. Alaska has told me that if I have this PIN lock removed I would be responsible for any future account fraud. They would rather put the burden of fraud management on their customers than implement common sense security measures in their systems.
#10261	27-Nov-25	Seattle Times	Chaz12345		I had the same issue with Alaska. When I called customer service person told me it was partially my fault. How I have no idea. In addition a flight I had booked with miles for my daughter was cancelled (they were leary about fraud again) although she is listed as a traveler in my profile —they cancelled anyway and I had to rebook for additional miles. Took a few calls to get the extra miles required to rebook flight returned. Then shockingly someone accessed my account again. I don't care about the miles as much as all the info in that account... passport info nexus card info... you name it. Alaska has a problem. They need to fix it. Class action lawsuit needed.
#10262	27-Nov-25	Seattle Times	CD	500,000	Alaska flyer since the Golden Samovar and gold bar giveaways days here. I recently had about 500000 miles stolen from my Atmos account I was alerted by an Alaskan email congratulating me for my upcoming trip. Like others I was on customer server phone for hours and finally found a chat bot that referred me to a fraud unit. I sent them the requested material and got a case number and have not heard back in weeks. Alaska: This is Reference#: 11XXX439 please call me or email at the numbers and address I sent you and let us get to the next steps. You should easily be able to find the stolen tickets cancel them and refund my mileage. ALSO I agree with others that your IT is so busy keeping your flight systems running I would guess that they have little time for mileage fraud. SUGGESTION: Outsource your fraud hunting to the banking partner that issues your credit card they have fully staffed fraud units with the computer tools and expertise to quickly find the fraudsters responsible. I look forward to hearing from you. Regards customer since early 1980.

Ref #	Date	Platform	Username	Miles Stolen	Comment
#10263	27-Nov-25	Seattle Times	BlueLakeDawg		Time for a two factor authentication Alaska? My miles disappear and you will have to reimburse me. Should all be treated like real money.
#10259	27-Nov-25	Twitter	NettePot	50,000	Watch your emails if you have AlaskaAir points!! 50k points redeemed by a scammer and customer service is off for thanksgiving. Congrats to whomever got a free flight on me!
#10264	28-Nov-25	Facebook	HM		This also happened to me last week. I made the mistake of logging out of my app thinking it was a glitch and then was locked out entirely and couldn't change my password. I had to call Alaska. They fixed it and refunded my points but they told me that if it happens again they will not refund a second time. They don't have MFA and they don't allow special characters in passwords. It's like they are begging for more fraud. Super sketch!
#10265	28-Nov-25	Reddit	BiggusDickusRoman		This happened to me over the summer as well. When I called to report it Alaska acted like they were doing me a favor by crediting the miles and telling me I'd now have to call a human with my PIN for any future redemptions. It would be so simple to modernize with 2FA but if it costs them a penny they just won't do it.