

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).
