Testimony of

John Breyault
Vice President of Public Policy, Telecommunications, and Fraud
National Consumers League

on

"Aviation Cybersecurity Threats"

Before the
United States Senate
Committee on Commerce, Science, & Transportation

September 18, 2024

Introduction

Good morning Chair Cantwell, Ranking Member Cruz, and distinguished members of the Committee. My name is John Breyault and I am the Vice President of Public Policy, Telecommunications, and Fraud at the National Consumers League. Founded in 1899, the National Consumers League ("NCL") is the nation's pioneering consumer and worker advocacy organization. Our non-profit mission is to advocate on behalf of consumers and workers in the United States and abroad.[1] On behalf of the NCL, I would like to extend our sincere appreciation to the Committee for giving me the opportunity testify. Today, I will address the serious impacts cybersecurity incidents in the aviation industry have on consumers and urge the Committee to ensure that consumers are not left bearing the costs of these events.

I. Recent Incidents Have Highlighted the Need for Action to Strengthen Cybersecurity Defenses and Reduce the Risk to Passengers

When cybersecurity incidents occur in the airline industry, consumers are often the ones who suffer the most. Flights are delayed or canceled, personal information is compromised, and families can find themselves stranded for days without recourse.

Recent incidents are emblematic of this impact, underscoring how interconnected airline systems are and how an error in one sector can create a cascading effect across the industry, harming millions of passengers.

Last month, a cyberattack on Seattle-Tacoma International Airport resulted in significant disruptions, affecting critical infrastructure including the baggage system, terminal screens, check-in kiosks, airport website, and even communication

[1] For more information, visit www.nclnet.org.

systems such as phone and email.[2] While larger airlines operating at Sea-Tac, such as Delta and Alaska Airlines, suffered fewer consequences, smaller carriers like Frontier, Spirit, Sun Country and all international airlines were among those especially affected because they do not have their own dedicated systems within the airport. Staff at affected airlines were forced to handwrite boarding passes and luggage tags for passengers and manually sort bags to their proper gates and baggage claims. This led to delays in both departing flights and bags arriving at their destinations.[3]

On July 18, a faulty update affecting CrowdStrike clients, including airlines, led to global system crashes, affecting an estimated 1.4 million passengers.[4]nearly 5,200 were canceled on the first day alone.[5] Delta Air Lines canceled 7,000 flights over a five-day span.[6] Families were left stranded, with one family in Seattle reportedly losing more than $7,500 while trying to rebook flights and cover lodging costs.[7]

While the CrowdStrike outage was not caused by malicious actors, hackers did reportedly take advantage of the chaos caused by the incident. They launched phishing attacks trying to trick people into downloading malware, divulging security credentials, or making financial payments. Fake websites arose fraudulently

---

[2] Kapko, Matt. "Seattle Airport Targeted in Cyberattack over Labor Day Weekend." *Cybersecurity Dive*, 5 Sept. 2024, www.cybersecuritydive.com/news/seattle-airport-cyberattack-labor-day/725772/.
[3] Brenda, David. "SeaTac Airport Outage Is Ongoing: Here's What Travelers Should Know." *Washington State Standard*, 27 Aug. 2024, https://washingtonstatestandard.com/2024/08/27/seatac-airport-outage-is-ongoing-heres-what-travelers-should-know/.
[4] Weston, David. "Helping Our Customers Through the CrowdStrike Outage." *Microsoft Blog*, 20 July 2024, https://blogs.microsoft.com/blog/2024/07/20/helping-our-customers-through-the-crowdstrike-outage/; Oxford Economics. "CrowdStrike Update Grounds Thousands of Flights." *Oxford Economics*, July 23, 2024, https://www.oxfordeconomics.com/resource/crowdstrike-update-grounds-thousands-of-flights/.
[5] Whitmore, Geoff. "The CrowdStrike Outage Is Still Impacting Airlines." *Forbes*, 22 July 2024, www.forbes.com/sites/geoffwhitmore/2024/07/22/the-crowdstrike-outage-is-still-impacting-airlines/.
[6] Draper, Kevin. "Delta Airlines Still Recovering from CrowdStrike Outage." *The New York Times*, 13 Sept. 2024, www.nytimes.com/2024/09/13/travel/crowdstrike-outage-delta-airlines.html.
[7] Tran, Louie. "Seattle Family Stranded Multiple Days after Delta Cancels Flights amid CrowdStrike Outage." *KIRO 7 News*, 14 Sept. 2024, www.kiro7.com/news/local/seattle-family-stranded-multiple-days-after-delta-cancels-flights-amid-crowdstrike-outage/CFNOKCMRGRB5FNL2ZIUVW5ZW5A/.

impersonating CrowdStrike. CrowdStrike also disclosed that hackers were circulating a malicious ZIP file largely targeting Latin American customers.[8]

Cyber threats are not confined to American air carriers. A 2021 data leak at Air India allowed cyber attackers to access systems for more than three weeks at the carrier's Atlanta data center, affecting approximately 4.5 million customers.[9] A May 2020 hack of British carrier EasyJet compromised the email and travel details of around 9 million customers, and the credit card details of more than 2,000 of them.[10] And a 2018 breach at British Airways stemming from a third-party cargo handler affected nearly a half million customers, with almost 250,000 individuals having their names, addresses, payment card numbers, and CVV numbers taken.[11]

Government aviation safety agencies are not immune to cyber incidents either. In early 2023, a contractor inadvertently deleted critical files while updating a database for the Federal Aviation Administration ("FAA"), causing a nationwide ground stop. More than 10,000 flights were delayed and over 1,300 were canceled, once again highlighting the fragility of airline infrastructure to human error and cyber vulnerabilities.[12] Although the FAA has since implemented backup systems to

---

[8] DeNardis, Laura. "Is Global Tech Infrastructure Too Vulnerable? Professor Responds to CrowdStrike. Microsoft Outage," Georgetown University, 25 July, 2024, https://www.georgetown.edu/news/ask-a-professor-crowdstrike-outage/

[9] "India's Massive Cyberattack Hits Airline Operations." *BBC News*, 22 May, 2021, https://www.bbc.com/news/world-asia-india-57210118; Sinha, Saurabh. "Air India Data Breach: SITA Says Cyber Attackers Accessed Some Systems for 22 Days at Atlanta Centre." *The Times of India*, 22 May, 2021, https://timesofindia.indiatimes.com/india/air-india-data-breach-sita-says-cyber-attackers-accessed-some-systems-for-22-days-at-atlanta-centre/articleshow/82864982.cms.

[10] Holton, Kate. "EasyJet Cyberattack Hits Operations." *Reuters*, 21 July 2024, www.reuters.com/article/easyjet-cyber-idUSFWN2D10F5/.

[11] Information Commissioner's Office. *British Airways Penalty Notice*. 16 Oct. 2020, www.ico.org.uk/media/action-weve-taken/mpns/2618421/ba-penalty-20201016.pdf.

[12] Shepardson, David *et al*. "U.S. FAA Says Flight Personnel Alert System Not Processing Updates after Outage." *Reuters*, 11 Jan. 2023, www.reuters.com/business/aerospace-defense/us-faa-says-flight-personnel-alert-system-not-processing-updates-after-outage-2023-01-11/.

reduce the risk of such failures, the incident illustrates how vital resilient systems are for maintaining public trust and ensuring consumer protection.[13]

II. Cyber Vulnerability of Airline Rewards Programs Is of Particular Concern to Consumers

While cyber events that disrupt flights generate headlines, the vulnerability of airline rewards programs has the potential to affect even more consumers.

As billions of dollars worth of points flow in and out of mileage programs annually, rewards programs are increasingly seen as easy pickings by hackers. The value of unused miles sitting in passengers' rewards accounts is staggering. According to a 2018 McKinsey report, more than 30 trillion frequent-flier miles were sitting unspent in accounts. That was enough to let almost every airline passenger in the world redeem miles for a free one-way flight.[14] Other estimates put the value of unredeemed miles for U.S. airlines at a lower, but still significant valuation. According to ValuePenguin, a consumer research website, the top five U.S. airline loyalty programs ended 2020 with a combined balance of $27.5 billion in unused loyalty program miles, up $2.9 billion from 2019.[15]

Unsurprisingly, all of those unused miles are an attractive target for bad actors. Between the fourth quarter of 2023 and the first quarter of 2024, bot attacks on airline accounts increased 166%, according to cybersecurity firm Arkose Labs.[16] The

---

[13] Heilweil, Rebecca. "After 2023 Outage That Paused Flights Nationwide, FAA Now Has Backup System." *FedScoop*, 21 Sept. 2024, https://fedscoop.com/after-2023-outage-that-paused-flights-nationwide-faa-now-has-backup-system/.

[14] Saxon, Steve and Spickenreuther, Thorsten. "Miles Ahead: How to Improve Airline Customer Loyalty Programs." *McKinsey & Company*, 10 Oct. 2018, www.mckinsey.com/industries/travel-logistics-and-infrastructure/our-insights/miles-ahead-how-to-improve-airline-customer-loyalty-programs.

[15] Greenberg, Peter. "Airline Loyalty Programs Getting Harder to Redeem Frequent Flyer Miles." *CBS News*, 20 June, 2022, www.cbsnews.com/news/airline-loyalty-programs-getting-harder-to-redeem-frequent-flyer-miles/.

[16] Arkose Labs. "The Wiretap: Hackers Want Your Airline Miles." *Arkose Labs*, 2 July 2024, www.arkoselabs.com/latest-news/the-wiretap-hackers-want-your-airline-miles/.

Loyalty Security Alliance, a travel industry group, estimates that successful hacks of rewards accounts have increased by 30-40%.[17] Experts state that roughly 1% of airline point redemptions are fraudulent, with total losses amounting to about 3% when associated costs, such as staff time and the refunding of points to some customers are included.[18]

Stolen airline miles fuel a thriving market on the dark web and other black markets where buyers redeem stolen points for gift cards or by purchasing airline tickets. Some of the hacked accounts are used to sell discounted airline tickets to the public on websites that are made to resemble legitimate travel agencies.[19]

The airlines need to do a better job of securing consumers' valuable miles accounts. Despite the well-known attractiveness of airline rewards to hackers, U.S. airlines have been inconsistent in their efforts to secure these accounts. Basic account security tools, like multi-factor authentication ("MFA"), that are commonplace on other sensitive accounts, like those for online banking, are not available to all passengers. While American Airlines began phasing in MFA in 2023,[20] it appears that United and JetBlue only began implementing MFA in recent months.[21] Neither Southwest nor Delta appear to offer MFA for their customers' rewards accounts.

---

[17] "Hackers Are Now Coming For Your Airline Miles And Hotel Points," *Forbes*, June 28, 2024, https://www.forbes.com/sites/jeremybogaisky/2024/06/28/airline-miles-hotel-points-hacking/.
[18] Bogaisky, Jeremy. "Hackers Are Stealing Airline Miles and Hotel Points, and Banks Aren't Coming to Your Rescue." *Forbes*, 28 June 2024, www.forbes.com/sites/jeremybogaisky/2024/06/28/airline-miles-hotel-points-hacking/.
[19] Bogaisky, Jeremy. "Airline Miles, Hotel Points Hacking: What Travelers Need to Know." *Forbes*, 28 June 2024, www.forbes.com/sites/jeremybogaisky/2024/06/28/airline-miles-hotel-points-hacking/; Bischoff, Paul. "How Much Are Stolen Frequent Flyer Miles Worth on the Dark Web?" *Comparitech*, 15 Nov. 2018, www.comparitech.com/blog/information-security/how-much-are-stolen-frequent-flyer-miles-worth-on-the-dark-web/.
[20] Leff, Gary. "American Airlines Rolling Out Required Multifactor Authentication to Access AAdvantage Accounts." *View from the Wing*, 20 June 2023, https://viewfromthewing.com/american-airlines-rolling-out-required-multifactor-authentication-to-access-aadvantage-accounts/.
[21] "2FA Finally Available." *Reddit*, April 2024, www.reddit.com/r/unitedairlines/comments/1c6jbko/2fa_finally_available/; WandrMe. "Status Update." *X* (formerly Twitter), 15 Sept. 2024, https://x.com/WandrMe/status/1803891483441008787

To make matters worse, airline miles accounts are not covered by any of the consumer protections that safeguard consumers' money in other contexts, such as FDIC insurance or the Electronic Fund Transfer Act's anti-fraud protections. The Internet is littered with stories of consumers whose rewards accounts have been hacked and who then must spend hours on the phone with airlines and other rewards providers to try and get their miles back.[22]

III. Recent Incidents Are Part of a Troubling, Industrywide Trend

The cyber incidents mentioned above may have been isolated, but taken together, they are part of a larger, growing trend. Ransomware attacks, in particular, are a widespread and increasing concerns for stakeholders in the aviation sector.

A recent report from cybersecurity consulting firm Bridewell found that 55% of civil aviation organizations were targeted by ransomware in the past 12 months. Of these, more than four-in-ten (41%) said that loss of data was one of the primary consequences and 38% pointed to operational disruption. More than a quarter (28%) said the financial losses from paying a ransom were a consequence of the attacks.[23]

---

[22] Henderson, Clint. "My AAdvantage Account Was Hacked — Here's What I Did Next." *The Points Guy*, 19 Apr. 2024, www.thepointsguy.com/news/hacked-aadvantage-account/; Adams, Kurt. "What to Do If Your Points or Miles Are Stolen." *Going*, 5 Apr. 2024, www.going.com/guides/points-miles-stolen; Sweet, Joni. "Hackers Can Steal Your Frequent Flier Miles—How to Protect Your Travel Loyalty Accounts." *Frommer's*, 12 May, 2023, www.frommers.com/tips/airfare/hackers-can-steal-your-frequent-flier-mileshow-to-protect-your-travel-loyalty-accounts; "Hackers Stealing Hard-Earned Travel Loyalty Points." *Central Oregon Daily News*, 31 July, 2024, www.centraloregondaily.com/news/consumer/hackers-stealing-hard-earned-travel-loyalty-points/article_d6a77a14-4f67-11ef-9e51-933d75667c96.html.

[23] Bridewell Consulting. *US CNI Research Report 2024: Cyber Security in Aviation*. 12 Aug. 2024, https://insights.bridewell.com/l/838563/2024-08-12/bq8xv/838563/17234559391WNSYJDg/US_CNI_Research_Report_2024__Cyber_Security_in_Aviation.pdf.

Boeing's Chief Security Officer Richard Puckett last year noted that ransomware attacks on the aviation supply chain jumped 600% in the past year.[24] One notable attack in 2023 targeted Boeing with a $200 million ransom demand.[25] The Transportation Security Administration ("TSA") cited "persistent cybersecurity threats against...the aviation sector" when adopting emergency amendments to certain security programs last year.[26]

The threats described above are not unique to the airline sector. While ransomware attacks targeted 55% of civil aviation organizations in the last 12 months, this compares favorably with other critical infrastructure sectors. For example, another survey by Bridewell found that over the same time period, 78% of financial services firms, 76% of firms in the rail sector, 71% of federal government organizations, and 60% of firms in the energy sector had experienced ransomware attacks.[27]

This finding is supported by similar data from the World Economic Forum, finding that among critical infrastructure sectors targeted by cybercrime activity, healthcare is most affected, followed by financial infrastructure, telecommunications, and then transportation.[28]

---

[24] Boynton, Christine. "Cybersecurity Threats in Aviation: Bolstered Efficiency and Geopolitics." *Aviation Week*, 20 April, 2023, www.aviationweek.com/air-transport/airlines-lessors/cybersecurity-threats-aviation-bolstered-efficiency-geopolitics.
[25] Vicens, AJ. "Boeing Confirms Attempted $200 Million Ransomware Extortion Attempt." *CyberScoop*, 8 May 2024, www.cyberscoop.com/boeing-confirms-attempted-200-million-ransomware-extortion-attempt/.
[26] Transportation Security Agency. "TSA Issues New Cybersecurity Requirements for Airports and Aircraft." 7 Mar. 2023, www.tsa.gov/news/press/releases/2023/03/07/tsa-issues-new-cybersecurity-requirements-airport-and-aircraft.
[27] Bridewell Consulting. *US CNI Research Report 2024: Cyber Security in Aviation*. 12 Aug. 2024, https://insights.bridewell.com/l/838563/2024-08-12/bq8xv/838563/17234559391WNSYJDg/US_CNI_Research_Report_2024___Cyber_Security_in_Aviation.pdf.
[28] Joshi, Akshay. "Cybercrime Target Sectors: Latest Cybersecurity News." *World Economic Forum*, 24 Apr. 2024, www.weforum.org/agenda/2024/04/cybercrime-target-sectors-cybersecurity-news/.

IV. Action to Spur Cybersecurity Investment Would Benefit Passengers

There have been some limited efforts to prompt additional investment in the aviation sector's cybersecurity resiliency, but more remains to be done.

For example, Section 395 of the Federal Aviation Administration Reauthorization Act of 2024 directed the FAA Administrator to convene a Civil Aviation Cybersecurity Rulemaking Committee within one year of enactment. The committee will be tasked with making findings and recommendations on cybersecurity standards for civil aircraft, aircraft ground support information systems, airports, ATC mission systems, and aeronautical products and articles.[29] Last year, the Transportation Security Administration rolled out new rules that require airports and operators to develop cybersecurity plans and obtain TSA approval of the plans. This follows on the heels of TSA rules directing airports and airlines to designate a cybersecurity coordinator, report cybersecurity incidents to the federal government within 24 hours, develop cyber incident response, and conduct vulnerability assessments.[30]

Industry bodies, such as the International Air Transport Association, also play a key role in developing cybersecurity standards for the aviation industry.[31] In the U.S., industry groups, led by Airlines for America, have been at the forefront in advocating for greater harmonization of cybersecurity regulations.[32]

---

[29] FAA Reauthorization Act of 2024. Sec. 395. https://www.congress.gov/bill/118th-congress/house-bill/3935/text

[30] Starks, Tim. "U.S. Government Debuts New Cyber Rules for Aviation Sector." *The Washington Post*, 8 Mar. 2023, www.washingtonpost.com/politics/2023/03/08/us-government-debuts-new-cyber-rules-aviation-sector/.

[31] International Air Transport Association. *Cyber Security in Aviation: Industry Position 2023*. IATA, 2023, www.iata.org/contentassets/f23f6fa53f6b4dff8178bf88102c9f09/acysec-industryposition-2023.pdf.

[32] The White House. *Cybersecurity Regulatory Harmonization RFI Summary*. June 2024, ("In their responses, Airlines for America (A4A) and the Association of American Railroads (AAR) advocated for adopting standardized cybersecurity frameworks to ensure that regulation

While these efforts are laudable, no amount of cybersecurity investment can prevent all incidents that impact passengers. It is for these reasons that NCL urges the U.S. Department of Transportation ("DOT") and Congress to take additional steps to reduce the harm that cybersecurity incidents cause to consumers. Specifically:

- Congress should pass comprehensive national data security standards legislation. NCL has long supported such legislation to give consumers a baseline of protection for the data that they share with industry, including with airlines;

- The value of airline rewards should be protected from fraud. Just as consumers are not liable when bad actors compromise their credit and debit card accounts and run up charges, so too should airlines be required to replace airline miles lost to cyberthieves; and

- Congress should explicitly codify DOT's authority to promulgate delay compensation rules and ensure that the forthcoming rules allow consumers to obtain cash compensation if an airline cybersecurity incident results in a significant delay or cancellation.

Conclusion

Chair Cantwell, Ranking Member Cruz, and members of the committee, we are grateful for your continuing work to protect consumers and for holding this hearing. On behalf of the National Consumers League, thank you for including the consumer perspective as you consider these important issues.

---

improves cybersecurity outcomes, not merely increases compliance costs.") www.whitehouse.gov/wp-content/uploads/2024/06/Cybersecurity-Regulatory-Harmonization-RFI-Summary-ONCD.pdf.