Follow Us on Twitter

April 19, 2012

Credit Card Fraud: Corporate Accounts – University Accounts

Several agents have again confirmed that compromised credit cards are being used for tickets that appear to be for their corporate account. (See ARC's fraud alert dated Dec. 23, 2010 on our fraud prevention pages at https://www.arccorp.com/support/fraud-prevention.jsp) In 2010 ARC warned agents about this type of scheme – one using the guise of an agent's corporate account to book and issue tickets using compromised credit cards. These non-face-to-face transactions are issued for immediate international departure, typically to and from West African airports, but could depart from any non-U.S. gateway.

Recently fraudsters either contact an agency directly or through an after-hours call center. He or she may claim an affiliation (e.g. employee, student, faculty) with a corporate (recently university or educational) account in an attempt to access the online booking tool or to convince an agent to issue a ticket ("social engineering" fraud).

A fraudster may also send emails that appear to be from university/educational email domains to convince you that he or she is affiliated with the corporate account. (Review ARC's credit card red flags on our fraud prevention pages at https://www.arccorp.com/support/fraud-prevention.jsp.)

Always review corporate account transactions, and do not assume that a ticket is legitimate simply because it originates from a "known" customer. You may also want to consider additional training for responses to after-hours requests for access to the online booking tool, password resets, etc. Assign someone to review all ticketing in your GDS daily, including weekends and holidays. **The current and previous days' bookings should be reviewed daily for:**

- Spikes in sales (cash and credit sales)
- Immediate (same or next day) departures
- Changes in a corporate client's usual travel patterns (e.g., same or next day departures, international departures, etc.)
- Use of unknown credit cards
- Unusual origins or destinations
- High-dollar tickets
- High-risk itineraries (e.g., international departures, especially LOS, ABJ, ACC, CMN)

What to do if you identify some of these changes in patterns or suspect compromised credit cards:

- Take immediate action to confirm passenger names and credit cards with your corporate account.
- Act quickly to properly void unconfirmed corporate tickets through your GDS to obtain the ESAC code from the carrier's e-ticket database.
- Cancel (do NOT refund) return segments of the ticket that may have been used outbound to reduce losses.
- If a corporate booking tool was used, determine how access to may have occurred.

Follow Us on Twitter 

- Review online booking tool rules and settings with each corporate account to identify and minimize vulnerabilities.
- Contact ARC's Fraud Prevention department for important follow-up information at fifp@arccorp.com or (703) 816-8137.

More on current schemes, fraud prevention and credit card transaction red flags can be found at https://www.arccorp.com/support/fraud-prevention.jsp.

About ARC:

As the financial backbone of the U.S. travel industry, ARC enables commerce among travel agencies, airlines, and travel suppliers, and offers them secure and accurate financial settlement services. About 16,000 travel agencies and 190 airlines make up the ARC network. In 2011, ARC settled more than $82 billion worth of transactions between travel sellers and airlines. ARC also supplies transactional data to organizations, facilitating better business decisions through fact-based market analyses. Established in 1984, ARC is headquartered in Arlington, Va. For more information, visit www.arccorp.com.

Contact:
Need to report fraud? Have questions about fraud?
☎+1 703.816.8137
+1 703.816.8138
fifp@arccorp.com

3000 Wilson Boulevard, Suite 300
Arlington, VA 22201-3862