



[Follow Us on Twitter](#)



July 12, 2012

Beware! Fraudsters Posing as Employees or Corporate Reps

Please read the following information and educate your staff and after-hours call centers. Recent schemes have involved over \$770,000 in compromised credit card transactions.

Unsolicited Corporate Account Scheme

Someone contacts you claiming to represent a talent or entertainment company that is in need of a travel agent for international airline travel (mostly for intra-South America). Once you become suspicious of the volume of tickets, credit cards and international departures, it may be too late. One travel agency discovered that it had issued more than \$160,000 worth of tickets using compromised credit cards. *Overall, around \$400,000 in compromised credit card transactions has been attributable to this scheme.*

What to consider as high risk:

- Non-local company
- Third-party transactions – Representative, passenger, cardholder are not the same person
- A company email account from a free provider like Yahoo, etc., instead of a company domain
- International departures, mostly South American airports like BOG, LIM, EZE, GRU, for immediate departure
- High-dollar tickets
- Use of multiple credit cards

Existing Corporate Account Scheme

Someone contacts you claiming to work in the South American office of one of your existing or previous corporate accounts and needing tickets for international employee travel (mostly for intra-South America). You are actually expecting his business because you have received a (fraudulent) call or email advising you that this person would contact you for tickets. *Over \$80,000 in compromised credit card transactions has been attributable to this scheme.*

What to consider as high risk:

- Third-party transactions – Representative, passenger, cardholder are not the same person
- Name or domain misspellings – adding or subtracting a letter, number or symbol
 - Fernando.aguilar@xyzcorporation-**au**.com instead of Fernando.aguilar@xyzcorporation.com
- International departures, mostly South American airports like BOG, LIM, EZE, GRU, for immediate departure
- High-dollar tickets
- Use of multiple credit cards

Spoofing Corporate Account Emails and Social Engineering Scheme

Someone contacts you claiming to be with your corporate account and stating that he is currently out of town but wants to purchase airline tickets. This person then sends you an email appearing to be from the account's domain with the details about passengers, itineraries and credit cards. You verify that the person is indeed with the account, and the request for tickets is fulfilled. *Since April 2012, more than 35 agencies have issued over \$290,000 worth of compromised credit card transactions due to this scheme.*



[Follow Us on Twitter](#) 

What to consider as high risk:

- Name or domain misspellings – adding or subtracting a letter, number or symbol
 - Johhsmith@abccuniversity.edu instead of Johnsmith@abcuniversity.edu
- An additional email address (the fraudster's), from a free provider
 - Johhsmith@abccuniveristy.edu (drekosk45@gmail.com)
- Immediate departures from international airports, mostly West African airports like LOS, JNB, ACC
- Unfamiliar corporate credit cards or use of multiple credit cards
- Third-party transactions – Representative, passenger, cardholder are not the same person
- Initial ticket request followed later in the day or next day by requests for multiple tickets for immediate international departures
- Changes in corporate account's typical ticketing – airports, carriers, class of service, average ticket price, etc.

What to do if you identify one of the above situations or suspect compromised credit cards:

- Take immediate action to confirm passenger names, employee and credit cards *directly* with your corporate account or the employee requesting tickets.
- Take immediate action to confirm a genuine cardholder's authorization through the credit card issuer.
- Act quickly to properly void transactions with confirmed compromised credit cards through your GDS to obtain the ESAC code from the carrier's e-ticket database.
- Contact ARC's Fraud Prevention department for important follow-up information and more ways to identify possible compromised credit cards 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.