Unsolicited Corporate Account Scheme

A fraudster is calling travel agents and independent contractors stating that he represents a building company (or engineering/moving company, etc.) in need of a travel agent to fulfill their travel needs. The first tickets are often for domestic travel, followed by international departures. Once you become suspicious of the number of tickets and credit cards being used as well as the international departures, it may be too late. Credit cards may already be compromised. Even though you have obtained a credit card authorization code, your agency can be held responsible if the real cardholder rejects the sales as fraudulent.

What to consider as high risk:

- New corporate account approaching you to do international tickets for immediate departure
- Third-party transactions (passenger and cardholder are not the same)
- The so-called company website domain may look legitimate, but additional pages are not developed or under construction
- The website/domain is only a few months old
- International departures (mostly to/from South American airports, i.e., BOG, LIM, EZE, GRU)
- Use of multiple credit cards

Consider using ARC's Red Flags list to determine the risk before you issue tickets. To find the Red Flags list, click the Best Practice tab on the Fraud Prevention space on the My ARC homepage. Provide a copy of the Red Flags document to each of your front line staff, including full/part-time employees and independent contractors.

If you suspect such a scheme and want assistance to assess the risk, contact ARC's fraud prevention team to at 855-358-0393 or fifp@arccorp.com.

Another alert follows on the next page.

Criminals Pretending To Be From Well Known International Entities

Agents continue to receive emails from prospective customers who pretend to be from a well known, international company or entity associated with foreign governments (e.g., consulates, companies promoting foreign tourism or business opportunities, etc.). The email seeks a travel agent to fulfill their requests for international airline ticketing (currently for South America departures from BOG and EZE). The criminal sets up a fake domain to look like his or her emails are coming from the well known company. He or she may use most of a real domain name and add a dash or underscore. The fraudster will provide photoshopped/fake passports, driver's licenses and credit cards.

Before you issue tickets for an unsolicited international corporate account, you may want to contact ARC's Fraud Prevention Team, since we may be able to immediately advise you of potential or confirmed fraud.

What to consider as high risk:

- Non-local company approaching you to do international tickets
- International tickets (South American airports, such as BOG, LIM, EZE and GRU, or African airports, such as ACC, DKR and ABJ) for immediate or next-day departures
- Third-party transactions (caller, passenger and cardholder are not the same)
- Extensions in email addresses of a well known international company, e.g., using a dash, such as visitmexico-**us**.com instead of visitmexico.com
- Newly set up websites rarely belong to a well established international company, or you may find that the domain was set up in a different country than the international company requesting tickets. Verify the domain address, especially those with extensions, e.g., visitmexico-us.com, through whois.com to determine where and when the site was created.
- Use of multiple credit cards
- Driver's license/passport/credit card copies sent to you appear fuzzy and contain errors, e.g., using GI instead of GA for Georgia on a driver's license.
- Credit cards may not be signed.

What should you do if you suspect compromised credit cards? 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 more ways to identify possible compromised credit cards and important follow-up information at fifp@arccorp.com,
(703) 816-8137 or (855) 358-0393.