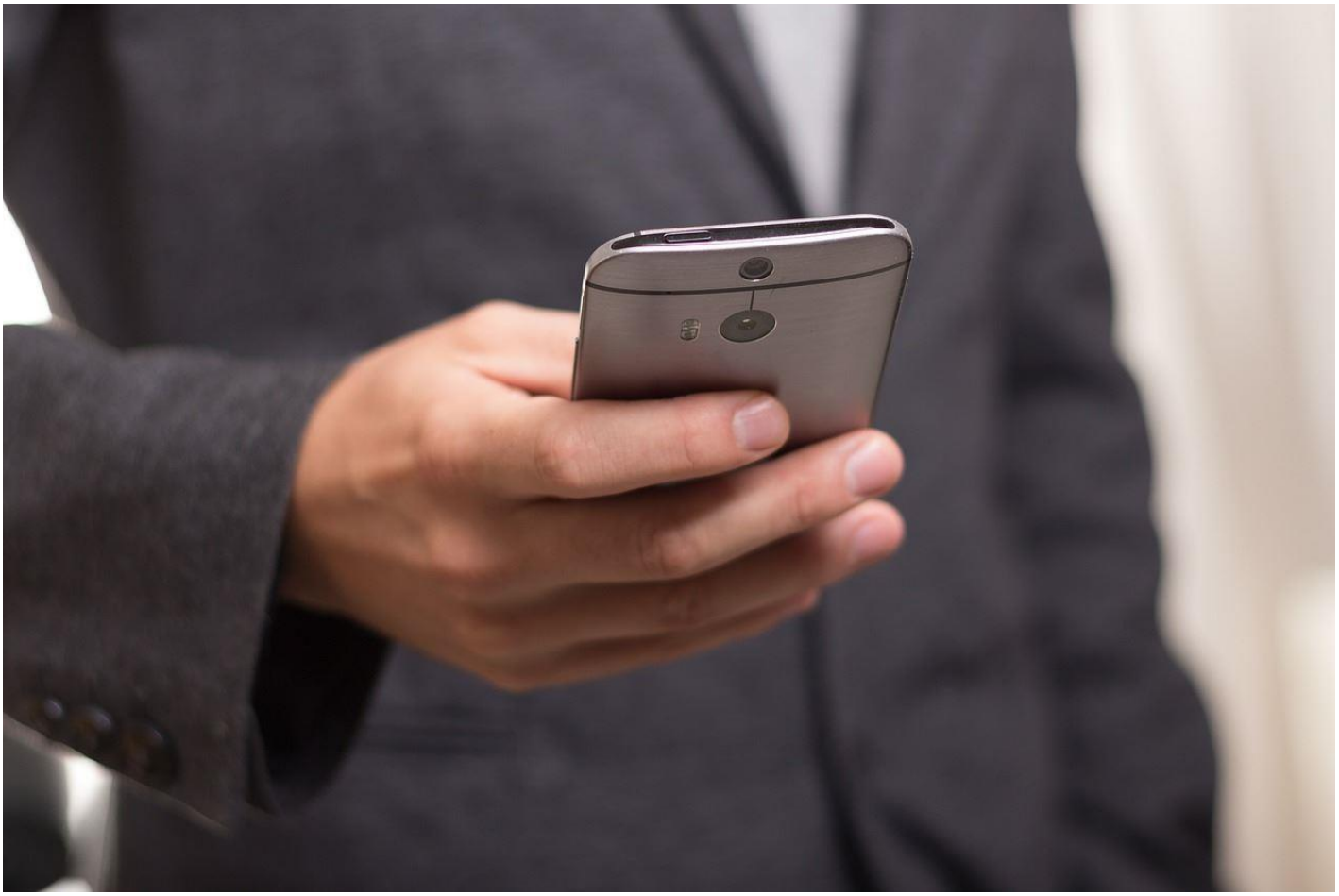
Guest Column: Fraud Prevention For Travel Agents, Part 1: Red Flags

by Emily Peters, with additional content contributed by ARC / April 26, 2016



In the past six months, I've spent innumerable hours trying to track down a fraudster who scammed a independent travel professional out of thousands of dollars.

The client seemed innocent enough: a doting son who had purchased a pair of first-class tickets to Europe as a gift for his parents. He approved the charge in writing, even sent in a photocopy of his driver's license. Sounds legitimate, right?

Wrong.

Though our story resulted in a chargeback that should have been indefensible, there were a few boxes left unchecked by the agent. With credit card fraud on the rise, it's more important than ever for travel entrepreneurs to know how to protect their business.

What is fraud?

Fraud is malicious or criminal deception intended to result in personal or monetary gain. In legal speak, it can also be understood as "false enrichment," meaning someone getting

money/not paying for something they should have by pulling a fast one on you, the agent.

In the travel industry, fraud is commonly perpetrated by “clients” purchasing travel products using stolen credit cards or issuing chargebacks (denying charges on their credit card) for products that they did actually use. Sometimes, fraud can even mean someone breaking into your GDS to book travel products without your knowledge or steal sensitive personal information.

Smells phishy: Red flags to watch for in initial contact

With the advent of the Internet, traditional “walk-in” travel customers are few these days. Fraud, therefore, naturally increases simply due to your inability to meet every client in person. With this in mind, proceed with caution whenever you receive new travel requests from an unfamiliar source. Any combination of the following scenarios should raise immediate suspicion:

- First point of contact is via e-mail, a form through your website, or a TTY service (for the hearing impaired)
- Client or passenger name is new to your agency
- The cardholder’s credit card, driver’s license, or passport can only be faxed/e-mailed because cardholder can never be present at the agency location (tricky for home-based agents, but always ask!)
- E-mail requests contain obvious spelling errors
- Caller ID shows the client as non-local, or no Caller ID information is displayed at all
- Caller claims to be a representative from a GDS or ARC and starts asking for your personal information/credentials
- Client can only be contacted via phone with a non-local area code
- Client uses fictitious U.S. address or phone number (Google everything!)
- Client can’t call you back OR you can only ever leave a message

In the travel industry, fraud is commonly perpetrated by 'clients' purchasing travel products using stolen credit cards or issuing chargebacks (denying charges on their credit card) for products that they did actually use.

Red flags: Fraudulent clients

Even if the initial contact seems innocent enough, keep on your guard. Other red flags that may reveal themselves during your qualification process. Here are a few of the most common:

- Client uses a religious/medical title (“Pastor Robert” or “Doctor Smith”) or religious premise (missionary work) to establish credibility or empathy
- Last-minute bookings
- Highly flexible travel schedule or budget
- Client doesn’t quibble over the price
- Client can’t or won’t fill out a credit-card authorization form
- Client has no local address
- Flights originate outside the United States
- Flights are international-to-international
- Client references airport codes instead of city names (e.g. asking for LAX to LOS instead of Los Angeles to Lagos, Nigeria)
- Passenger is not the cardholder
- Client can’t or won’t verify the billing address of the credit card being used
- Client uses a single credit card to book several routings, travel dates, and passenger last names
- Client uses multiple credit cards to pay for the trip
- Client offers multiple credit cards for payment if first card is rejected
- Client purchases high-priced tickets for a third party (bingo—this was the case with the culprit mentioned above)

Red flags: Fraudulent access to your GDS

Not all fraud comes in the form of a sneaky client; some comes from skilled fraudsters gaining access to your GDS or client information. If you are a GDS user and/or have sensitive client information on your computer, beware the following:

- “Phishing” e-mails containing attachments or links that entice you to click for additional information or to update your GDS credentials/profile (NEVER open attachments or click on links from unknown sources!)
- Calls from someone pretending to represent your GDS or ARC, requesting your login information or agency credentials like your IATA number
- Calls from anyone claiming to be in the travel industry requesting access to your client list (for marketing purposes, etc.)

We believe that when it comes to protecting your agency and your pocket book, paranoia is your friend. Committing the above red flags to memory will drastically reduce your risk of fraud.

Come back for the next part of our three-part fraud prevention series, where we’ll explore the latest fraud schemes and best practices for fraud prevention.

Emily Peters is the business development manager of Montrose Travel

Guest Column: Fraud Prevention, Part 2: Recent Schemes And Best Prevention Practices

by Emily Peters, with additional content contributed by ARC / May 03, 2016

This is part 2 in a three-part series.

Fraud's the name, prevention is the game. In Part 1 of our series, we touched on the numerous "red flags" that should immediately trigger your suspicion when dealing with clients. Today, we'll explore recent schemes and best practices for preventing fraud.

Recent fraud schemes

- Travel in and out of Africa, Bogota, Panama, Ecuador, Dominican Republic, and Dubai. The above are current hot spots for travel-related fraud across the world. To protect our agents, for example, we disable the ability to book flights to or from Africa on their websites. That certainly doesn't mean you should reject the next client looking for a safari. But you should always refer back to the red flags for safety's sake.
- Friendly fraudsters. Clients who establish a warm rapport with you (the agent) and never quibble about price or ask for four-star treatment, but then issue a chargeback as soon as travel is complete.
- GDS login credentials. As we mentioned in our last installment, a common scheme involves fraudsters e-mailing you for additional information regarding your GDS. Their email

will contain a link (that you should never, ever click!) to a phony login page or a questionnaire. You enter your GDS credentials, thinking you're logging into your GDS or updating information—but instead they've snagged your credentials and can book products without your knowledge or consent.

- Social engineering call. In this scheme, a caller claiming to represent ARC (Airlines Reporting Corporation) or your GDS asks for your GDS or agency credentials.
- Phony advance reservation. Recently, clever fraudsters have booked a week or two in advance of travel (making their reservation less suspicious). Yet as soon as they receive the confirmation email, they call the airline directly and change the departure date to the next day or within a few days—and then they can check in for the flight. (If it's international, they can do this if their flight is within two days). Once these kinds of changes are made, they can be very difficult to cancel. Some airlines will help and some will not, so be on your guard.
- Holiday travel scheme. Fraudulent bookings often spike during the holidays. With Memorial Day around the corner and the summer holidays beyond that, be sure to carefully monitor your online bookings and keep a close eye on red flags to avoid entrapment.

Though fraudsters frequently change their tactics to avoid detection, popular schemes have lasting shelf lives. Keep up with the latest schemes by signing up for ARC's fraud alerts here.

Fraud prevention best practices for your business

Maybe you've been there—glancing over your banking statement only to realize someone has been swipe-happy somewhere with your card. Fraud affects us all, but a little well-incorporated paranoia can prevent you from becoming a victim.

- Never, never, never click on links or open attachments in an e-mail. When in doubt, hover your cursor over a link *without clicking*. This will reveal a pop-up with the real website address associated with the link. Here, try hovering over this link: GDS Login. This seems like common sense, and it is—but you'd be shocked to know how much fraud results from careless clicking.
- Use malware, spyware and/or a firewall on your computer to prevent viruses from stealing information.
- Regularly update your computer's operating system to keep security tight.
- Use complex passwords to access your GDS account and change then every three months.
- Never store client credit card or passport information directly on your computer. Use a secure CRM option that will encrypt client information.

Best practices when dealing with a client

Dig into who your clients really are. Ask where they learned about you, and how they found your name, e-mail, or website. Don't be afraid to ask if they're local to the area and how long they've lived here. If something doesn't feel right, politely decline their business; it's as easy as saying, "I don't believe I'm the best fit for your needs."

- Never skip your full qualifying process, even if you're dazzled by a potentially fat commission check. Go through the paces each time, every time.

- Always have a client fill out and submit a written credit-card authorization form that clearly outlines the amount to be charged. *Do not* rely on approval via texts or phone calls.
- Always get copies of the front and back of a client's credit card and photo ID.
- Always check cards for signs of counterfeit (see below!).
- If you use a GDS, monitor your bookings for suspicious activity every day. If you have a website, do the same with anything booked on your site.
- Do not book any flights departing within seven days or costing more than $1,000 without interviewing the client in depth.
- Immediately void or cancel any suspicious bookings. If you do not have the ability to do this yourself, contact your host agency (if you have one) to handle it for you.

Identifying phony credit cards or personal identification

By now, you're probably picking up on a theme: the best way to combat fraud victimization is knowledge. It befits any travel professional to know the basics of how to spot fake credit cards or photo IDs. It's not always easy, but it's worth the extra trouble (trust us). Here are a few tips:

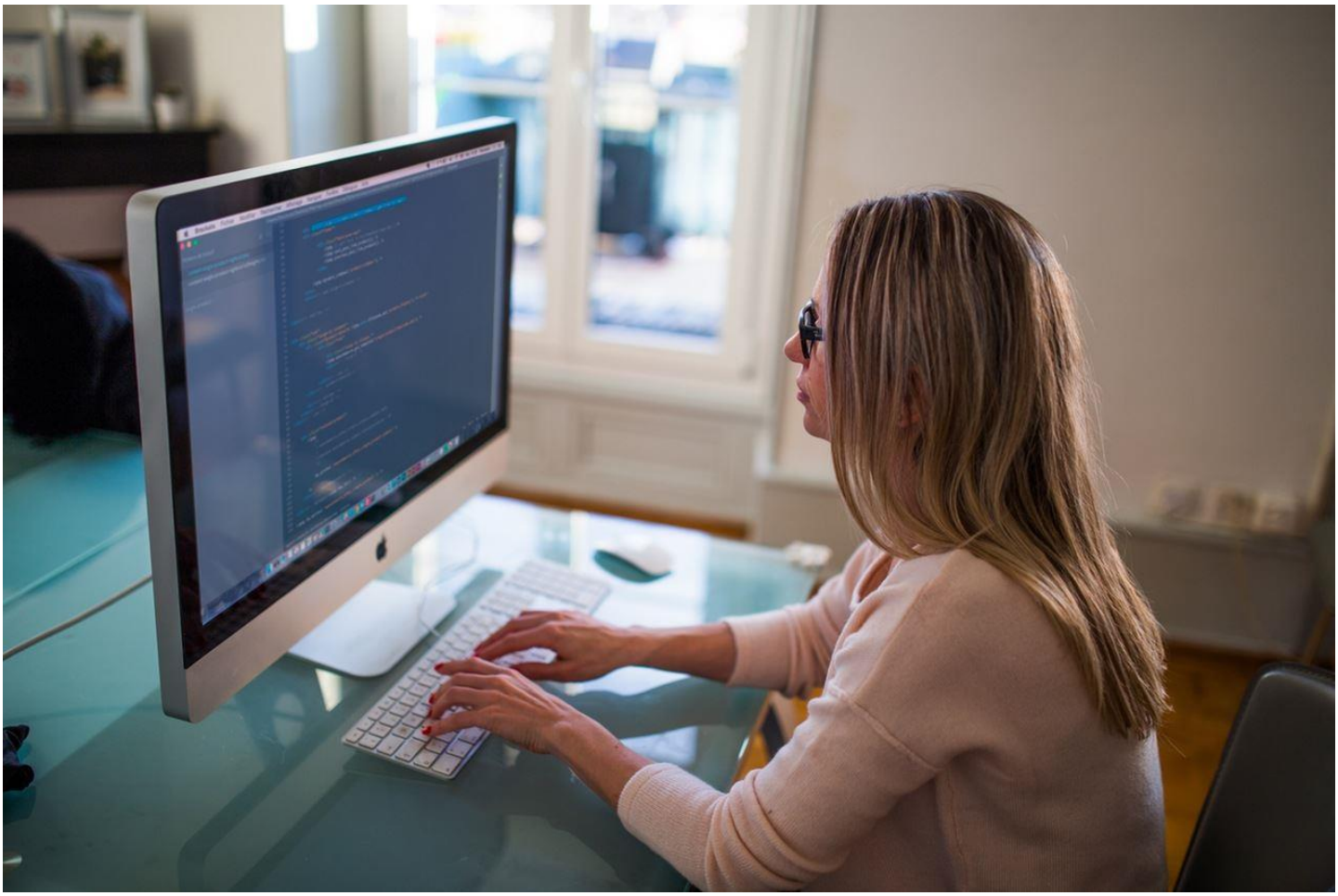
- Check the BIN Number: Verify that the credit card BIN number (the first six digits of any credit card number) is associated with the correct country and issuer. For example, if a client resides in the United States, the credit card number should not be Canadian. A good resource to check BIN numbers is www.Binlist.net; it will tell you the bank issuer, country, card type (debit/credit), and brand (Visa, MasterCard, etc.) of the card in question.
- Check the raised print: Verify that the raised, printed name on the front of the card corresponds to the name on back of the card. For example, "John Smith" in raised print on the front should not read "Mike Jones" (Or rather, senoJ ekiM) on the back.
- Check for oddities: Make sure photo IDs and copies of credit cards have no visible discrepancies, such as oddly cropped photos or suspicious watermarks. ARC recommends that you enlarge the front and back of any copies you receive and search the small print for awkward phrasing, misspelled words, etc.
- Check the signature box: Make sure the printed name on the front of the card matches the signature on either the front/back of card. ARC also recommends that you not accept unsigned cards or cards that contain erasures (white blotches) in the signature lines.

Need more tools? Here are some suggestions from ARC:

IDcheckingguide.com – compare copies of driver's licenses to current and past licenses issued by each state
Whitepages.com – reverse phone directory
Googlemaps.com – check out addresses to see if someone's home address is really a vacant lot, strip mall, etc.
Emailage.com (arccorp.com) to see when an email address was established
Contact ARC's fraud prevention team at fifp@arccopr.com or (703) 816-8127 to talk to a fraud prevention analyst

Guest Column: Fraud Prevention Part 3, What To Do When You're a Victim of Fraud

by Emily Peters, with additional content contributed by ARC / June 15, 2016



Part 3 in a three-part series.

Fraud's the name, prevention is the game. In Part 1 of our series dealt with numerous "red flags" that should immediately trigger your suspicion when dealing with clients, Part 2 explored recent schemes and best practices for preventing fraud. Today, we'll explore the worst-case scenario: what to do when you're a victim of fraud.

Document your actions

Before you can effectively combat fraud as a crime, you need to have a record of what you've done vs. what your client has done. Gather all your documented actions (e-mails, phone calls, texts, faxes, etc.) as well as any client responses.

Report the problem to your host

Montrose Travel has hosted independent contractors for more than 40 years and has

more than 500 ICs, each with his or her own client base. Yet, we've never had to make a claim against our Errors & Omissions insurance. How can that be?

The secret is in swift communication between our ICs and our support team. We counsel each and every one of our independent travel professionals to immediately report chargebacks, instances of credit-card fraud, or debit memos. As a host and a retail travel agency, we have deep resources to help battle these problems. If you find yourself the victim of fraud, do not delay in giving the details to your host agency. Don't go it alone.

Report the problem to ARC

ARC (Airlines Reporting Corporation) is an excellent resource for all things fraud-related in the travel industry. It trains regularly on fraud prevention—and the more you report fraudulent activity, the better ARC can help law enforcement to track, identify, and prosecute criminals. Report any suspicious phishing emails or fraudulent activity directly to ARC at fifp@arccorp.com. If it's GDS-related, report the issue to your GDS help desk as well.

Report the problem to the authorities

Filing a report with your local, state, and/or federal authorities will provide you with leverage later on, especially if you wind up in a legal dispute.

File a suit against the fraudster

With any luck, you'll have been able to protect yourself well enough that going to court is not necessary. However, if that is not the case you can consider filing a suit against your fraudster. Small claims suits are generally for damages amounting to less than $10,000 and can be done (albeit with a lot of legwork) without a lawyer. Damages beyond that should involve the help of a lawyer, or can be split into multiple small claims suits depending on the situation. Our suggestion: let hiring a lawyer be a final resort. Legal fees can often wind up being more expensive than the amount you're suing for.

Whether preventing credit card fraud, chargebacks, or the evil debit memos we all dread, you can play defense in many ways when it comes to fraud protection for your travel agency. We hope this fraud prevention series has helped give your agency and pocketbook the protection they deserve.

Emily Peters is the business development manager of Montrose Travel.