Reducing Fraudulent Transactions and Chargeback Agent Debit Memos

Credit fraud is a serious problem for airlines and travel agents alike

Jennifer Watkins, ARC's Director, Credit Card Services & Fraud Prevention and Christophe Kato, IATA's Head, Payment Services, discuss the trends in fraudulent Card Payment activities in our industry and how ADM reduction could be an indication of fraud prevention

What is the relationship between a Chargeback and an ADM?

Jennifer Watkins:
Some would say that there is a one-to-one relationship between chargebacks and chargeback ADMs. However, the difference is that with a chargeback there is an opportunity to provide supporting documentation to reverse it before an ADM is issued.

When data is presented to attempt to reverse the chargeback, a debit memo is only issued if the card brand determines that the liability still falls to the airline. In other words, the supporting documentation didn't provide enough evidence to prove that the actual cardholder authorized the transaction. Through this process, by addressing the chargeback fraud (also known as "friendly fraud") cases, the number of chargeback ADMs issued could be much less than the number of fraud chargebacks that occur.

Through the chargeback management process, the hope is that there will be a lot fewer chargeback ADMs than chargebacks. However, the ultimate goal is to eliminate unnecessary chargebacks before they are initiated.

Christophe Kato:
The chargeback is the transaction through which the issuer of the card 'claws back' from the acquirer the financial settlement he previously made for the purchase his cardholder made at the merchant.
Chargeback rules are set by the card scheme under which rules the purchase was made.
The acquirer lists in its merchant card acceptance agreement the provisions to pass the chargeback onto the merchant.
In turn, the ADM is the transaction through which the airline, who is the 'merchant of record' for the transaction, passes that financial loss onto the Travel Agent. ADM rules are set by IATA BSP provisions.

Do you think that the volume of Chargebacks in our sector have been impacted by the endeavors of the two Agency Debit Memo Working Groups (ARC & IATA) and how?

J.W:
Yes, because most chargebacks are due to fraud, I would argue that ARC's and IATA's efforts to educate agents about fraud prevention have had a big impact on reducing fraud that would have become chargebacks. Both of our organizations work year-round to educate agents on fraud in our industry, and we identify and integrate tools that agents can use to reduce fraud.

Another key factor that reduces debit memos related to chargebacks, that I believe is tied to the collaborative environment built through the Debit Memo Working Groups, is the fact that airlines are working more closely with, and on behalf of, agents to reverse chargebacks prior to issuing debit memos. This reduces the volume of debit memos issued, and ultimately reduces future chargebacks by fighting chargeback fraud (a.k.a., friendly fraud, or third-party fraud), and correcting bad cardholder behavior.

C.K:
In my work I really look only at card payment transactions and the issues that arise in connection with them.
The first thing I can say is that the 2 groups have truly broke ground by managing to identify the reasons behind those ADMs, which was the absolute pre-requisite to any action looking at improving the situation and reducing the number of instances leading to ADMs.
When I joined IATA in 2008, it was one of the first questions I asked, what was the volume of ADMs caused by fraud chargebacks and I quickly understood the information was simply not there.
The industry has come a long way, and we are now attacking the root cause of 'card fraud chargeback-caused ADMs'.

Are there any technologies or methods that help Airlines and Agents detect and prevent credit card fraud and how can they apply these mechanisms to protect their business from fraud?

J.W:
There are almost countless technologies and tools available for agents and airlines to plug into their transaction flows to evaluate the risk of credit card fraud. The challenge is identifying which tools to employ as part of a comprehensive fraud prevention strategy — and weighing that against the potential customer impact associated with some tools such as 3D Secure, Address Verification or Card Identification.

When it comes to fraud prevention tools, there are resources for every business regardless of the model or size. The options for validating cardholder identity and evaluating risk includes everything from sophisticated machine-learning tools, fraud-scoring tools that evaluate various risk factors, to home-grown systems and the use of free online tools. (A list of free fraud prevention tools is available on ARC's website: https://www2.arccorp.com/support-training/fraud-prevention/free-internet-tools/)

C.K:
Absolutely, there are many, but because of the peculiar set up of Agency card sales where the Agent operates on behalf of the airline, I feel that neither of the 2 parties ever felt fully in charge and, therefore, neither researched deep how they could improve things over time. There are 3 dimensions to look at:

First, making full use of the fraud prevention mechanisms proposed by the card schemes and that will say, along the approval of the authorization request, if the client knows the security code (which sits on the back of the card) and the cardholder billing address (this one does not work for all cards but it does for US, Canada and UK cards, that are the most defrauded all over the world)

Second, passing the transaction through the filter of a fraud detection tool that will spot details hinting it may be a fraud. One needs then to follow up on that alert and review the purchase to decide to let is stand or cancel it.

Those 2 sets of actions are meant to be conducted at the time of sale or right after, which means that they really reside in the hands of the Travel Agent.

And third, Airlines and Agents need to collaborate when a fraud chargeback hit, so that the airline stands the best chance to challenge it with success, because if it does, then there is no financial loss to assign.

In particular, the truth is that some abusive customers are tempted to take advantage of the sometimes too easy way to raise a dispute, in order not to pay their card purchases. It is only by combining:

- what the Agent and the airline know of the customer
- the way the client conducted and paid for the purchase
- how the service was delivered that airline and agent have the chance to challenge together what they think to be an abusive claim.

What are the different ways for the "Brick and Mortar" Travel Agents and Online Travel Agents to reduce exposure to credit card fraud?

J.W:

In the U.S. market, the risk of fraud in a face-to-face (card-present) environment is much lower than in a non-face-to-face (card-not-present) environment. That isn't to say that bad guys won't create counterfeit cards and present them to an agent. In a card-present environment the goal is to validate that the card is not counterfeit or stolen. The best way to do this is via a terminal with a chip card reader. The challenge in the U.S. market is that GDSs don't have credit card terminal capability. Therefore, the best practice is still to obtain an imprint of the card and a signature whenever possible. It can also help to request a photo ID from the cardholder and ensure the picture and names match. The challenge is that we constantly see counterfeit cards and counterfeit passports. The good news is that, to date, most fraudsters are not willing to present them in a face-to-face environment.

In an online travel agency environment, validating that the customer is the actual cardholder is more difficult and requires a more sophisticated set of tools that collects all kinds of data about the customer and the transaction. Fraud rings can operate online anywhere in the world, and they are good at maneuvering through a set of fraud prevention tools, so it is important to monitor and constantly change the strategy for stopping them.

C.K:
Both conduct the BSP card transaction in a nearly identical way, in the sense that the data they enter into the GDS for the creation of the card transaction is the same.
However, brick and mortar Agents have the opportunity to take a signed manual imprint of the card, something that may allow the airline to dispute successfully a fraud chargeback.
On the other hand, on-line Agents don't have this option but they are certainly familiar with the concept of 3DSecure to make Internet card transactions safer. 3D Secure is not yet supported in BSP but within a year's time we intend to change that, with the active collaboration of GDSs and Agents.

How would you describe the role that credit card merchants have in fraud detection?

J.W:
ARC defines the credit card merchant as the entity accepting the credit card. In the payment industry, the merchant is defined as the entity that has the merchant agreement with the card company. Regardless of how it is defined, there is opportunity for agents and airlines to work together to reduce fraud losses.

Fraud detection needs to happen at the point of sale, whether online, over the phone, or face-to-face. This is the opportunity to collect the data that validates that the cardholder is the actual cardholder and they are participating in the transaction. The credit card companies have identified various tools to help merchants do this, but it is up to the merchant to use those tools and more, at the point they are collecting information about the customer.

C.K:
The card accepting merchant is told very precisely by its acquirer, in the merchant agreement, when he is liable for fraud losses. Hence it is its duty to take action to protect itself from such losses, by making full use of the card scheme provided fraud prevention features, by using a fraud detection system and by developing the policies allowing him to challenge chargebacks with a chance of success.

In BSP card sales, that duty is split between airline and Agent because though the airline is undoubtedly the 'merchant of record', it does not conduct the card transaction at time of sale, the Agent does it on behalf of the airline.

How do you foresee the future of fraud prevention and how would it impact ADMs?

J.W:
The bad guys are constantly improving their techniques for perpetrating fraud. This means merchants must employ fraud prevention tools that are constantly evolving. Most large online travel agencies (OTAs) and airlines have developed sophisticated fraud prevention strategies. They are using tools like 3D Secure to authenticate the cardholder and employing machine learning to identify fraud online. This makes it harder for the bad guys to perpetrate fraud through these channels. My concern is that they

will move to agents and airlines that don't have the same sophisticated infrastructure in place — which is why it's so important for agencies of all sizes to implement tools and training to help detect and prevent fraud.

C.K:
Education, education, education. We know there always be hackers and fraudsters who can defeat the best. But the great majority are not geniuses, they are simply using ready-made tools and techniques. And there is no excuse to lose money to incompetent fraudsters, such as the one writing '*use of the cards in the list I emailed you, and if they don't work, just ask me for other card numbers'*. Don't smile, I have read such email exchanges between 'customers' and sellers.

Too many people still believe, and this is true of all retailers, it's not an issue specific to the travel trade, that securing an authorization approval code is a guarantee to be paid. Not it is not, not in the remote sale arena.

If you were using a chip and PIN terminal yes it could be true, but I can never say it enough, an authorization approval code does not guarantee you against fraud. You need to take other measures.

But it is not rocket science. The main thing is to be aware. Before fraud hits you and damages seriously your business. Then, as a professional, you know what to do or where to go to learn what to do.

What are the top industry best practices that are proving a successful fraud and chargeback reduction?

J.W:
I could talk about some of the sophisticated fraud tools that agents and airlines have employed, but for the agents we talk to every day, it comes down to educating agents about some common-sense red flags to look for. It includes putting processes in place in call centers to stop bad actors from manipulating team members into ticketing transactions using stolen card numbers. It's about identifying the level of risk an agency is willing to take, and developing a fraud prevention strategy around that.

The best advice for a smaller agency is to know your customer, which doesn't always mean actually knowing their customers personally, but knowing how their typical customers behave. When someone wants to purchase something outside that pattern, it is a red flag. For a slightly larger agency that is taking transactions from people they don't know, either online or over the phone, they may want to put some basic tools and procedures in place to confirm the customer's identity as the cardholder. For large agencies that process a high volume of transactions with unknown individuals from all over the world, they need to employ a more fulsome fraud prevention strategy to avoid taking losses due to fraud. (Section 6 of the ARC Industry Agents' Handbook includes best practices for card acceptance fraud prevention and is available on ARC's website: https://www2.arccorp.com/globalassets/iah/iah.pdf)

C.K:

Take any white paper or publication on fraud prevention, they are always aligned on their core message:

- Awareness first, which means setting a fraud prevention policy with clear KPIs (Key Performance Indicators) and responsibility for those assigned no less clearly.

  Don't worry about KPI being something complex, it can be as simple as measuring your fraud losses, understanding why you lost, and set an objective to reduce that number. And keep measuring on a regular basis, don't wait and pray for good news once a year!

- Take full advantage of all basic fraud prevention features provided by the card schemes:
  - Card security code (CVV2) match and mismatch response alongside an approval code
  - AVS (address verification service)
  - 3DSecure when relevant and when the actors in BSP are ready to support it
- Using a fraud detection system supported by clearly defined review policy stipulating what to do when a transaction is flagged as suspect.
- Cooperate closely with your business partners to reduce the volume of problems, rather than just looking to fraud as a loss to assign somewhere.
  This includes understanding what is needed to challenge chargebacks with a chance of success, including recognizing that card schemes have minute differences in their rules and policies, so make sure you stick by THEIR rules. Remember, they set the rules and we have to live by them
- Use feedback from good, and from bad experiences ('when you lost') in order to update your KPIs and policies
- Stay in touch with all work groups, forums and publications that will help you remain aware of what you should know

How effective are the real-time credit card fraud detection mechanisms and how can they help Agents and Airlines to get instant decisions before fraudsters can harm their business further?

J.W:
There are many tools in the marketplace that use real-time artificial intelligence. These tools are very effective at helping merchants confirm the good transactions therefore reducing friction to the customer, and immediately reject the transactions that are identified as fraud. The best tools either reduce or eliminate the need for people to further evaluate transactions.

There still isn't a silver bullet to eliminate credit card fraud, but as technology advances, many of the real-time credit card fraud detection systems are becoming increasingly effective. Thanks to these advancements, organizations are now able to reduce fraud to levels that were previously unattainable.

C.K:

There is today a large selection of providers proposing a very rich portfolio of services, with extensive experience and operating on all sales channels and in any geographical location. Everyone can find an offer tailored to its need, from a basic rule system installed in-house to the full outsourcing of fraud detection, all the way to calling your customers on your behalf and challenge them (in a professional way!) on suspect transactions and deciding on your behalf to cancel the transaction or let I stand.

This is done at time of sale or post sale, the risk appetite and the requirements of each entity will determine what is best, there is never a 'one size fits all' solution.

However, it is crucial to remember that merely buying a fraud detection service will not bring down fraud by itself, like, magically.

Such an investment must be the consequence of a clearly laid out fraud prevention policy. The tool, or service, is only a 'means to an end', it will deliver alerts as per the KPIs set by the user, and such alerts need to be 'worked on' by a review team assigned to this task and operating a clearly laid out 'review policy'.

Let me conclude by noting that fraud prevention is not a finite time project, because if you hit your KPIs and disband your fraud team…. the picture is going to change pretty fast. Fraud prevention is merely a cost of doing business and is part of normal and on-going operations. It was never and will never be a onetime effort that make a problem go away forever.