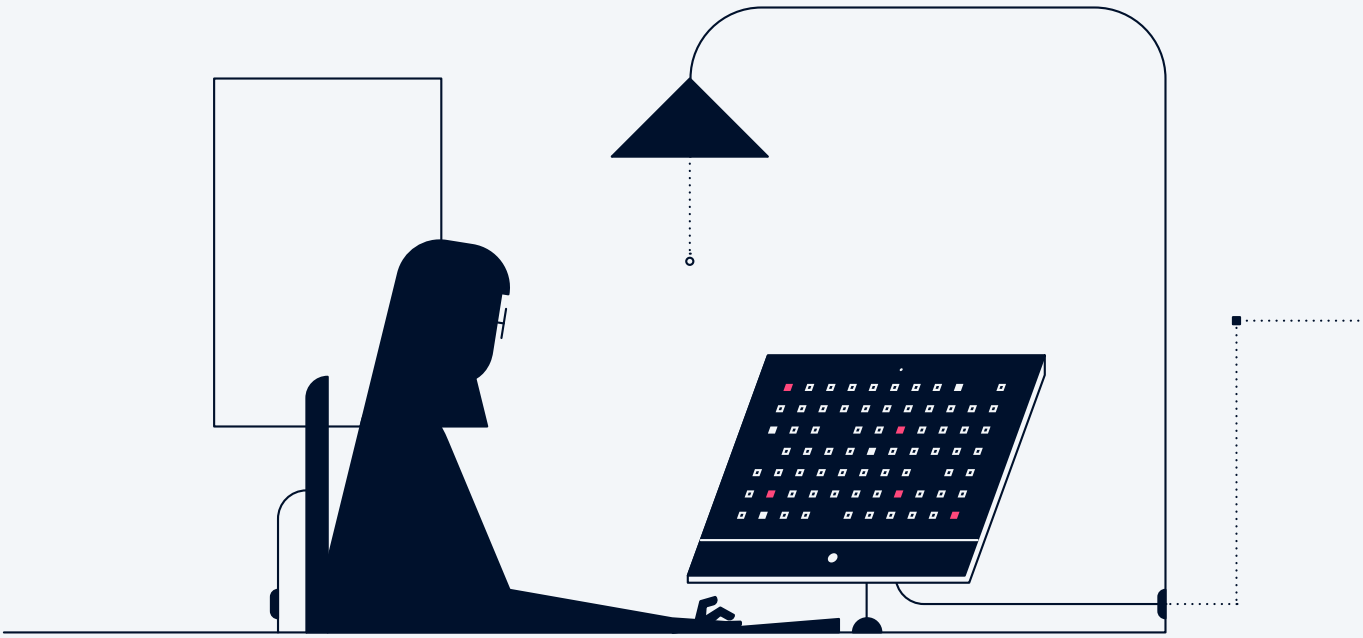
Version 3.1, 2020

Brazil

Fraud & Chargeback Manual

adyen

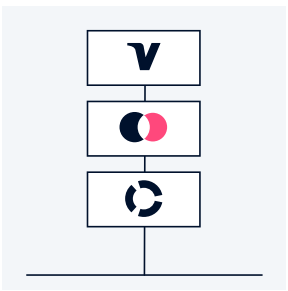
Contents



Objectives

One of Adyen's key missions is to help our customers reduce and control fraud and chargeback percentages. We are aware that this is a constant problem for many establishments and, in most cases, these two topics are related.

The purpose of this manual is to inform our customers regarding the potential consequences of excessive fraud and chargeback, which can lead to the imposition of fines by the brands, to encourage them to correct the problems.



Note 1

As an acquirer, Adyen works directly with brands with respect to fraud and chargeback programs. When Adyen acts solely as a gateway, it is the customer that defines which acquiring network will take on this role.

Introduction

This manual contains:

- The rules governing issuerbrands' fraud and chargeback programs;
- The practical aspects of the programs;
- The fines that may be imposed if fraud and chargeback problems are not corrected in a timely manner;
- The regulations related to fraud and chargebacks in the Latin American region.

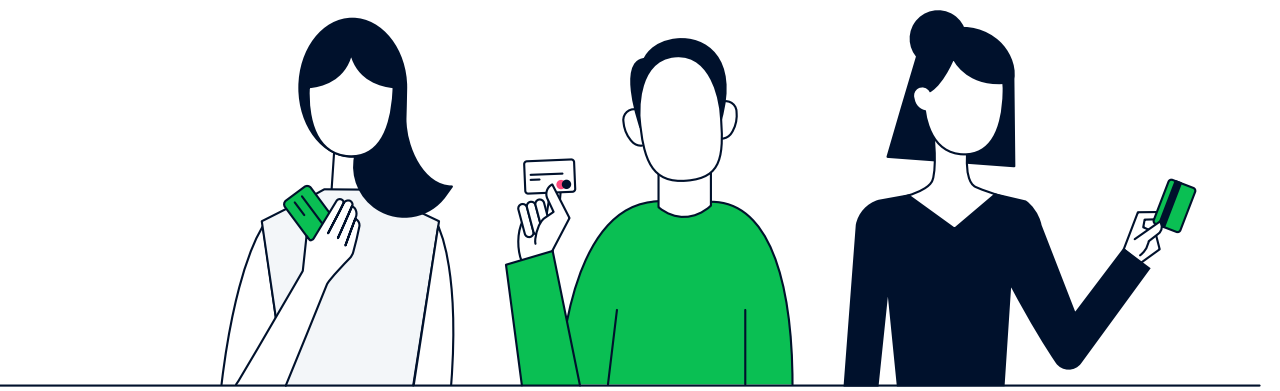
Note that each program is different and works independently of the others. Any changes to the programs are made by the brands themselves and are not managed by Adyen. It is important to note that each Merchant is responsible for monitoring the performance indices along with the brands, through reports on the CA or even internally. In cases where a substantial increase in the volume of disputes is detected, Adyen may, in due course, request further information in addition to an action plan to reduce these indices. Stay up to date by tracking our posts on adyen.com.

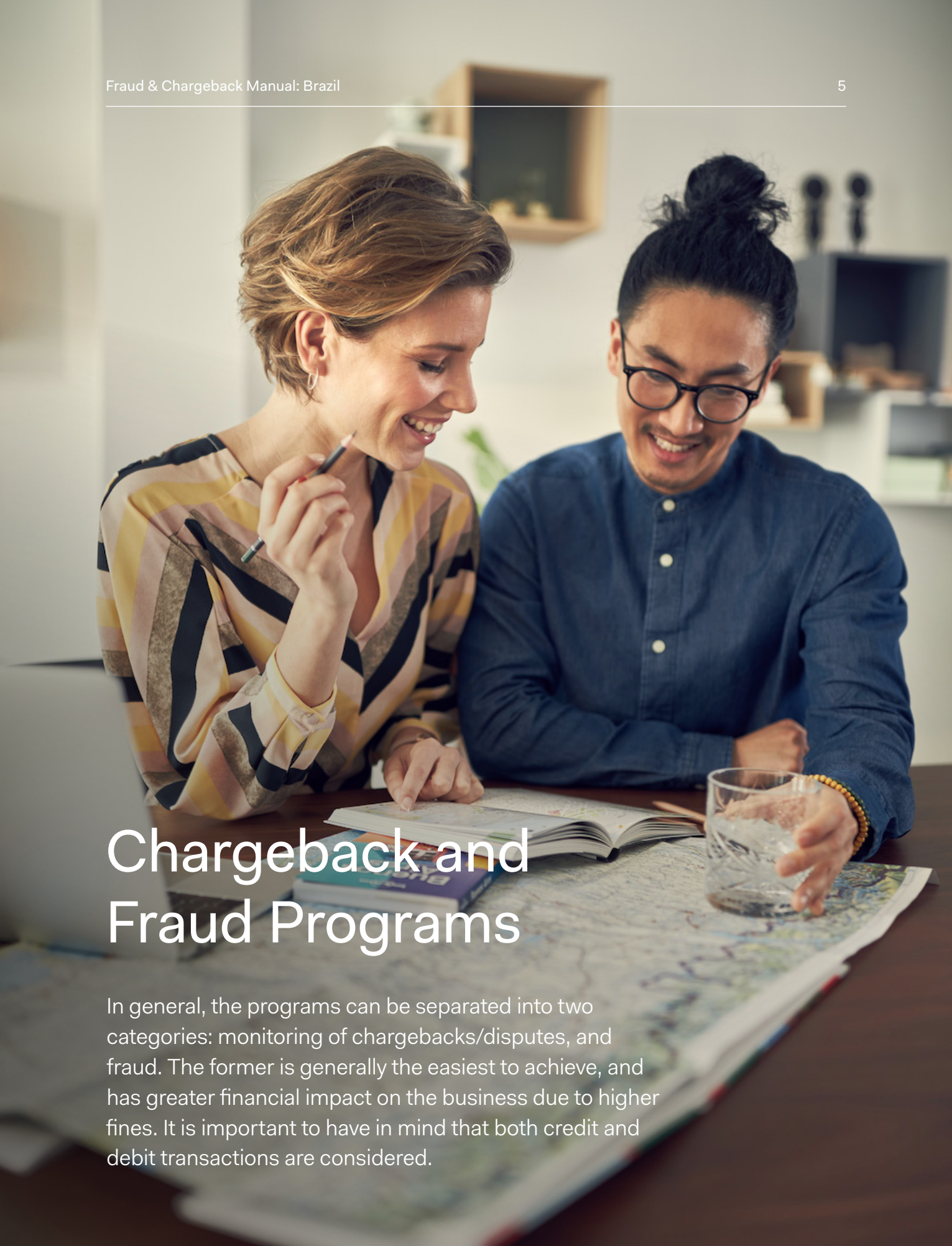
Note 2

Any penalties for non-compliance with the program rules are imposed by the brands on the establishment's acquirer (in this case Adyen). As agreed in the contract, Adyen subsequently charges the amount of those fines to the establishment in question.

Target audience

This is an informative manual intended for establishments that process payments in Latin America.





Chargeback and Fraud Programs

In general, the programs can be separated into two categories: monitoring of chargebacks/disputes, and fraud. The former is generally the easiest to achieve, and has greater financial impact on the business due to higher fines. It is important to have in mind that both credit and debit transactions are considered.

Chargeback programs are calculated individually by each brand, and dispute reports can be downloaded from the Adyen Dashboard. Its main objective is to ensure that commercial establishments maintain acceptable levels of chargebacks, regardless of their reason. Therefore, it is important to keep in mind that all chargeback notifications received, whether for fraud, commercial disagreement or non-delivery of goods, for example, will be considered.

Establishments that authenticate transactions through the 3Ds protocol with the issuers become liable for the chargeback, the so-called liability shift. Even in this situation, issuers may send a chargeback notification to the acquirer, but since Adyen has an automatic self-defense system, there is no need for action by the establishment when this occurs. It is important to note that even with liability shift, both fraud notifications and chargebacks of transactions authenticated by 3Ds will be included in the program calculation.

Below are the four main card brands in the Latin America region and their respective chargeback and fraud programs.

Glossary

Explanation of the basic concepts of fraud and chargeback

Excessive Chargeback Program – ECP:
Mastercard's main chargeback control program.

Excessive Chargeback Merchant (ECM):
Acronym for "establishment with excess chargebacks." It is Mastercard's first level chargeback program for establishments exceeding limits.

HECM: Acronym for High Excessive Chargeback Merchant, or establishment with high excess chargebacks. It is Mastercard's second level chargeback program for establishments far above limits.

VDMP: Acronym for Visa Dispute Monitoring Program.

VFMP: Acronym for Visa Fraud Monitoring Program.

Adyen Dashboard: Also known as Customer Area (CA), this is the tool through which the customer can have visibility of all their transactions and manage their payments easily and efficiently.

Liability shift: Transfer of responsibility for the chargeback from the establishment to the issuing bank.

Data Only: Type of transaction by the establishment whereby additional data is sent to the issuer for the purpose of assisting the approval of the transaction.

3DS: Safety protocol designed for brands to combat fraud. To confirm the payment, the buyer must perform an extra authentication step.

Fraud Notification: The notification sent from the issuing bank. This is a notification made by the issuer to indicate that the transaction shows signs of fraud. In cases where a transaction shows evidence signs of fraud, the issuer must report it on the brand's tool ex: Mastercard (Safe) Visa (TC40). The NOF does not generate any financial transactions on the merchant's agenda; it is strictly a NOTIFICATION.

Notification of Chargeback (NOC): Upon receiving the NOC from the issuer, we create a dispute on the Dashboard. The establishment has the option of whether or not to defend the dispute and is subject to receiving the chargeback debit.

Merchant ID: Unique identification number for the establishment. Also known as MID, this number is used by the brands to identify and relate a transaction to the correct establishment.

Basis point: A term used for percentage calculation (%). A change of 0.01% is the same as one basis point, for example.

MCC: Acronym for Merchant Category Code, i.e. the specific code used to classify the sector of an establishment. e.g.: transportation, restaurants, hotels and entertainment.

CNP: Acronym for Card Not Present, i.e. a transaction made without the presence of the physical card.

CP: Acronym for Card Present, i.e. a transaction made with the presence of the card.

Early Warning: Early warnings from the Visa Dispute Monitoring Program.

Standard Status: Standard Status of the Visa Dispute Monitoring Program.

Excessive Status: Excessive Status of the Visa Dispute Monitoring Program.

High Risk Status: High-Risk Status of the Visa Dispute Monitoring Program.

Soft descriptor: This is an additional text that will appear next to the establishment's name on the buyer's credit card invoice. This text can be defined in the store register or in the payment creation/pre-authorization request.

Mastercard Programs

Mastercard (ECP) – Excessive Chargeback Program

Mastercard's excessive chargeback control program is called ECP - Excessive Chargeback Program. It is automatically monitored by the partner company on a monthly basis, using the customer's MID (merchant identification) as the key to the calculation. This calculation is always based on the chargeback notifications received during the month, compared to the transactions captured in the previous month. The report for the month of March, for example, would compare the chargebacks received in February versus the transactions captured in January.

Figure 1

Potential Excess Chargebacks Fees and Fines

Program	Indexes	Potential fees and fines			
		Number of months over ECP tresholds	**Penalty applicable per month in violation of ECM limits (100-299 chargebacks and 150-299 Bases point)**	**Penalty applicable per month in violation of HECM limits (>300 chargebacks and >300 Bases Point)**	
Mastercard Excessive Chargeback Program (ECP)	ECM: Chargeback Rate (CTR) ≥ 1.5%; and Chargeback quantity ≥ 150 < 300 (in one month)	**Quantity**	**Penalty (BRL)**	**Penalty (BRL)**	**Issuer's recovery penalty**
		1	-	-	No
		2	4.750	4.750	No
		3	4.750	9.500	No
		4 to 6	23.750	47.500	Yes*
		7 to 11	118.750	237.500	Yes*
		12 to 18	237.500	475.000	Yes*
		19+	475.000	950.000	Yes*
	HECM: Chargeback Rate (CTR) ≥ 3%; and Chargeback quantity ≥ 300 (in one month)	*Issuer recovery fine applies 6.19 BRL per chargeback above 300 chargebacks. For example, an establishment with 500 chargebacks could potentially be fined 1,238.00 BRL in recovery fines (500-300 = 200 x 6.19 BRL = 1,238.00 BRL)			

Mastercard (ECP) - Program Calculation

Every month, Adyen calculates the chargeback rate (CTR) for all its customers. CTR is the number of chargebacks received in a month, divided by the number of transactions captured in the previous month (a CTR of 1% = 100 bps).

Figure 2

Example of CTR calculation in March

$$= \frac{\text{\# of February Chargebacks}}{\text{\#of January Settled Transactions}}$$

Mastercard (ECP) - Chargeback Monitoring Cycle

The chargeback monitoring cycle is divided into 2 scenarios:

1. . Excessive Chargeback Merchant (ECM)
2. High Excessive Chargeback Merchant (HECM)

Figure 3

Excessive Chargeback Establishment

	Excessive Chargeback Merchant (ECM)	High Excessive Chargeback Merchant (HECM)
Program Requirements	CTR ≥ 150bps Chargeback Quantity ≥100	CTR > 300bps Chargeback Quantity ≥300
Input Criteria	Two months over the limit, consecutive or not.	Two months over the limit, consecutive or not.
Output Criteria	Three consecutive months below the 150 basis point index (1.5%).	Three consecutive months below the 150 basis point index (1.5%).

Mastercard (ECP) - Remediation Program/ Program Exit

An establishment becomes an ECM if it has a minimum CTR of 150 basis points for two months (consecutive or not) and at least 100 chargebacks each month. In the case of HECM, the difference is in quantity: at least 300 chargebacks and an index greater than 300 basis points.

These classifications only change when the chargeback rate remains below 150 basis points for three consecutive months.

Mastercard (ECP) - Additional requirements for ECM and HECM statuses

Once an establishment has been identified as ECM and/or HECM for six months (consecutive or not), Mastercard may:

1. Advise the establishment on the action plan and the measures the acquirer should take or consider reducing the chargeback rate; and/or
2. Require the acquirer to participate in the Franchise Management Program at the cost of the acquireracquirer's expenses.

Exit from the program is only possible if the establishment manages to stay below the limits for three consecutive months.

Figure 4

Sample exit from ECM/HECM programs

Month	Status ECP	Penalty Amount
January	ECM (month 1)	0
February	No violation	0
March	ECM (month 2)	BRL 4.750
April	HECM (month 3)	BRL 9.500
May	No violation	0
June	No violation	0
July	No violation - audit ended	0

Mastercard (EFM) – Excessive Fraud Merchant

Fraud programs are calculated individually by each brand and can be viewed on the Adyen Dashboard. Only chargebacks with reasons related to fraud are considered in Mastercard's program.

Establishments that authenticate transactions through the 3Ds protocol with issuers become liable for chargebacks, the so-called liability shift.

However, even if they are held liable for chargebacks, issuers may send the chargeback notification to the acquirer. Since Adyen has an automatic self-defense system, there is no need for action by the establishment in this type of situation. It is important to note that even with liability shift, both fraud notifications and chargebacks of transactions authenticated by 3Ds are included in the program calculation.

Figure 5

Potential Excess Fraud Fees and Fines

Program	Indexes	Fees and potential fines	
		Number of months above the limits EFM	**Violation Fine**
Mastercard Excessive Fraud Merchant Program (EFM)	Fraud rate ≥ 0.5% ≥ 50,000,00 BRL on fraudulent transactions ≥ 1,000 transactions settled Transactions authenticated with 3DS and/or data-only are ≤ 10% of the total number of card not present transactions	1 2 3 4 a 6 7 a 11 12 a 18 19+	BRL 0 BRL 2,375 BRL 4,750 BRL 23,750 BRL 118,750 BRL 237,500 BRL 475,000

Mastercard (EFM) - Program Calculation

Mastercard's EFM entered into force globally on October 1, 2019. The program also takes into account the establishment ID (MID). Below are the four criteria for joining the EFM:

Figure 6

Potential Excess Fraud Fees and Fines

#	Criterion	Definition
1	At least 1,000 ecommerce transactions; and	
2	The total valueamount of 50,000 BRL or more in fraud chargebacks; and	**Mastercard Fraud Chargeback Motive Codes:** 4863: Cardholder does not Recognize - Potential Fraud 4837: No Cardholder Authorisation
3	Net fraud rate of 0.5% or more; and	**Net Fraud Rate:** Amount of fraud chargebacks received in a month divided by the number of transactions settled by Mastercard in the previous month (see example at the end of the brochure).
4	Transactions authenticated via 3DS and/or data-only when: Regulated countries account for less than 50% of the total volume of cards not present (CNP) Non-regulated countries account for less than 10% of the total volume of CNP	**Regulated countries:** Countries with legal or regulatory requirements for strong customer authentication. To date, there are no regulated countries in Latin America. **Non-regulated countries:** Countries without a legal or regulatory requirement for strong customer authentication, such as Brazil, for example. **Data-only flow:** The establishment provides additional information within the payment request to Mastercard to improve its risk score models. Note that in the data-only flow no strong customer authentication occurs and the responsibility for the chargeback remains with the establishment.

After joining the EFM, establishments then receive a deadline to exit the program, which occurs once they submit three consecutive months of results below the limit.

Figure 7

The table below shows how fines are reset:

Number of months in EFM	Fine per month (BRL)
1	0
2	2,375.00
3	4,750.00
4 to 6	23,750.00
7 to 11	118,750.00
12 to 18	237,500.00
Greater than 19	475,000.00

If an establishment is identified in both the Mastercard Excessive Fraud Merchant Compliance Program and the Mastercard Excessive Chargeback Program, only EFM penalties will be applied. If the company leaves the EFM, but still exceeds the ECP limit ECP, then the fines corresponding to the latter will be imposed.

Figure 8

Identification of the establishment in the Mastercard Fraud Excess Program (EFM)

Month of data	EFM criterion				Program Status	Penalties (USD)
	Settled transactions	Fraud Amount (USD)	Net Fraud Rate	% 3DS and/ or data-only		
November 19	9,372	23,462	0.75%	4.0%	No	N/A
December 19	15,124	50,009	0.64%	3.5%	1 - EFM	N/A
January 20	23,113	48,128	0.61%	10.5%	No	N/A
February 20	21,347	61,847	0.69%	7.8%	2 – EFM	N/A
March 20	19,853	64,127	0.56%	7.0%	3 – EFM	1,000
April 20	20,241	56,935	0.58%	9.1%	4 – EFM	5,000

Visa Programs

Visa (VDMP) – Excessive Chargeback Program

Visa's excessive chargeback control program is called VDMP, or Visa Dispute Monitoring Program. It is automatically monitored by the brand on a monthly basis, using the customer's soft descriptor as the key to the calculation. This calculation is always based on the chargeback notifications received during the month, versus the transactions captured in the month itself. We can use the reporting month of March as an example, which would compare the chargebacks received in February versus the transactions captured in February.

Figure 9

Visa (VDMP) - Potential Chargeback Excess Fees and Fines

Program	Indexes	Fees and potential fines
Visa Dispute Monitoring Program (VDMP)	**Early Warning:** Chargeback Rate ≥ 0.65% and Chargeback Quantity ≥ 75	No fines apply.
	Standard Status: Chargeback Rate ≥ 0.9%; and Chargeback Quantity ≥300	25.00 USD per chargeback (after the fifth month above the limit), whether consecutive or not, and additional fine of 25,000.00 USD and possible need for an external advisory/ review from the tenth month, consecutive or not, above the limits.
	Excessive Status: Chargeback Rate ≥ 1.8%; and Chargeback quantity ≥ 300 (in one month)	25.00 USD per chargeback already in the first month above the program limits and an additional fine of 25,000.00 USD, as well as possible need for an external advisory/ review from the seventh month, consecutive or not, above the limits.
	High Risk: Chargeback Rate ≥ 0.9%; and Chargeback Quantity ≥ 100 and be considered a high-risk establishment as classified in MCC's 5962, 5966, 5967, 7995, 5912, 5122, 5993	

Visa (VDMP) - Program Calculation

In the Brazilian market, the VDMP monitors international and domestic transactions. The current month's chargeback rate is calculated using the chargeback and transaction volume data for the same month.

Figure 10

Example of chargeback rate calculation for the reporting month of March:

$$= \frac{\text{\# of February Chargebacks}}{\text{\# of February Settled Transactions}}$$

In addition, for VDMP compliance purposes, Visa will include only the first 10 chargebacks for each unique card number per establishment per month.

Visa (VDMP) – Early Warning

Early warnings provide establishments with the opportunity to reduce chargeback levels before they are identified in the VDMP. Visa sends monthly notifications to establishments that have not exceeded the program limits but have surpassed 75 chargebacks and had a chargeback rate of 0.65% in the previous month.

Visa (VDMP) – Standard Status

In the VDMP, the establishment enters the standard program if it reaches or exceeds the following chargeback limits:

≥ 100 chargebacks, and Chargeback rate ≥ 0.9%

Deadlines and possible sanctions: In the standard status, the establishment receives a three-month deadline to reduce chargeback levels, during which no fine is charged. In the event that the establishment exceeds the limits for five months, Visa will impose fines as described below:

Figure 11

Example of Visa fines

Excessive Status

An establishment can enter the VDMP with excessive status under any of the following three criteria.

1. High-risk MCC in excess of the standard program limit, or

The following MCCs are classified as high-risk:

- 5122 – Drugs, Drug Proprietors, and Druggists Sundries
- 5912 – Drug Stores, Pharmacies
- 5962 – Direct Marketing—Travel–Related Arrangement Services
- 5966 – Direct Marketing—Outbound Telemarketing Merchants
- 5967 – Direct Marketing—Inbound Telemarketing Merchants
- 7995 – Gambling Transactions

2. Excessive rate and volume of chargeback; or

An establishment will be assigned excessive status if it reaches or exceeds the following chargeback limits:

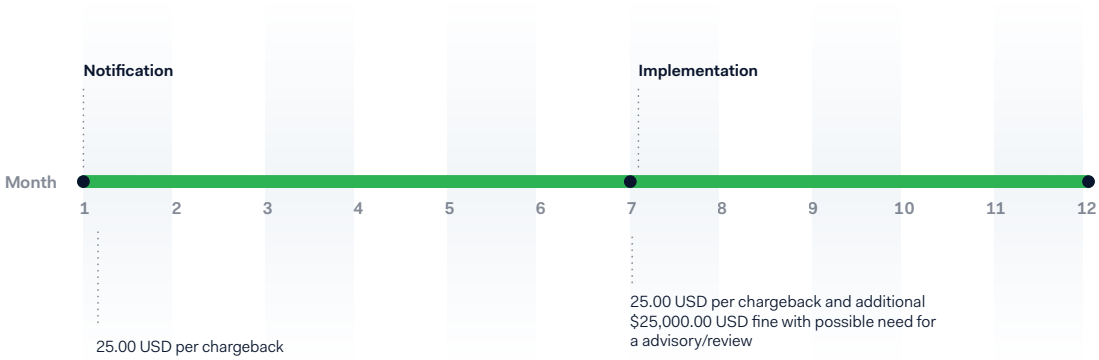
- ≥ 1,000 chargebacks, and
- Chargeback rate ≥ 1.8%

3. At Visa's discretion, establishments may fall into Excessive Status based on an analysis of establishment performance and inappropriate business practices (such as the use of abusive free trial policies, negative renewal options, etc.).

Deadlines and possible sanctions: Establishments will remain on the excessive status schedule until they keep chargeback levels below the standard status limits for 3 consecutive months.

Figure 12

Deadlines and possible sanctions



Correction/ Program Exit Criteria

The exit criteria are the same for Standard and Excessive statuses: the establishment must show results below at least one of the chargeback limits for three consecutive months.

In the event that the establishment succeeds in doing so for two months, but in the third once again exceeds the limits, the counting will be reset and resume in the month in which it is again below the limits.

Figure 13

Standard Status examples

Month	Chargeback Rate	Chargeback Quantity	Status	Penalty
June	1.60%	120	Standard – Month 1	N/A
July	1.28%	102	Standard – Month 2	N/A
August	0.88%	94	Below limits – month 1 of 3	
September	0.87%	102	Below limits – month 2 of 3	
October	0.92%	108	Standard – Month 3	N/A
November	0.95%	110	Standard – Month 4	N/A
December	0.88%	97	Below limits – month 1 of 3	
January	0.89%	88	Below limits – month 2 of 3	
February	0.85%	65	Below limits – month 3 of 3	

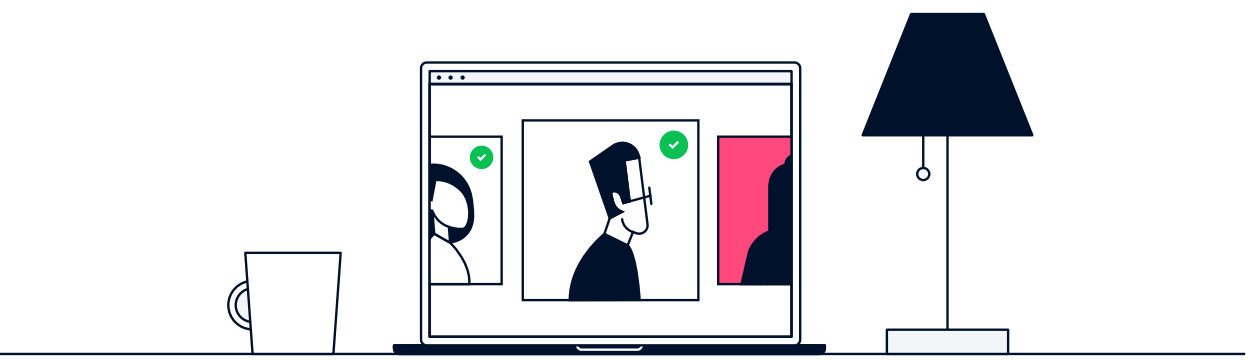
Here, the establishment managed to stay below the limits for two months (August and September), but in October it again exceeded them. At this time, the month counting went back to zero. It was only resumed in December, when the establishment once again managed to show results below the limit. As in January and February the results were also favorable (three consecutive months), the establishment managed to exit the program.

Figure 14

Excessive Status examples

Month	Chargeback Rate	Chargeback Quantity	Program Status	Penalty
October	1.78%	940	Standard – Month 1	N/A
November	1.77%	976	Standard – Month 2	N/A
December	1.85%	1,102	High Risk – Month 3	Applicable
January	1.92%	960	High Risk – Month 4	Applicable
February	1.70%	715	High Risk – Month 5	Applicable
March	1.38%	548	High Risk – Month 5	Applicable
April	0.89%	407	Below limits – month 1 of 3	
May	0.81%	302	Below limits – month 2 of 3	
June	0.75%	245	Below limits – month 3 of 3	

When the establishment exceeds excessive chargeback limits for the third month, it enters the High-Risk Program and, until it shows results below the standard limits again, it is subject to penalties.



Visa (VFMP) – Visa Fraud Monitoring Program

Figure 15

Visa (VFMP) - Visa Fraud Monitoring Program

Program	Indexes	Fees and potential fines
Visa Fraud Monitoring Program (VFMP)	**Early Warning:** Chargeback Rate ≥ 0.65%; and chargeback quantity ≥ 50,000.00 USD in 1 month	No fine is imposed. This is simply an early warning that the establishment needs to take the necessary steps to understand the root cause of the problem and reduce the percentage of fraud.
	Standard Status: Chargeback Rate ≥ 0.9%; and chargeback quantity ≥ 75,000 USD in 1 month	No fine is imposed, but the acquirer will be eligible for chargeback code 10.5 after the fourth month.
	Excessive Status: Chargeback Rate ≥ 1.8%; and chargeback quantity ≥ 250,000 USD in 1 month.	The acquirer will be eligible for chargeback code 10.5 from the first month and Between the first and third months, a 10,000 USD monthly fine will be imposed. Between the fourth and sixth month, a 25,000 USD monthly fine will be imposed. Between the seventh and the ninth month, a monthly fine of 50,000 USD will be imposed. As of the tenth month, a monthly fine of 75,000 USD will be imposed.
	High Risk: High-risk establishments classified in MCC's 5962, 5966, 5967, 7995, 5912, 5122, 5993	
Visa Fraud Monitoring Program — 3D Secure (VFMP-3DS) – US only	≥ 0.75% of 3DS authenticated transactions; and ≥ 7,500 USD in fraudulent transactions that have been authenticated (3DS) and reported.	No fine is imposed. However, the acquirer will be immediately eligible for chargeback code 10.5.

In Brazil, Visa monitors domestic and international transactions calculating fraud numbers for VFMP.

Fraud rate is calculated as follows: February Fraud Rate

Figure 16

February FSR Ratio

$$= \frac{\text{Total \$ amount of reported fraud in January}}{\text{Total \$ amount of sales in February}}$$

For VFMP compliance purposes, only the first 10 fraudulent transactions reported to Visa for each unique card number per establishment per month will be included. In addition, penalties associated with the identification of the VFMP will be ignored in the event that the establishment has already been identified in the VDMP with the sanctions applied in the specified month.

Globally, other regions that monitor domestic and international transactions are Brazil, Canada, Germany, the United Kingdom, and the United States.

Visa (VFMP) – Standard and Excessive Status

Similar to VDMP, VFMP has two categories: (1) Standard status; and (2) Excessive status, each with its own schedules and structures, as described below.

Figure 17

Visa (VFMP) - Standard and Excessive Status

	Fraud Rate	Fraud Value (in dollars)
Early Warning Limit	0.65%	50.000,00
0.65%	50,000	75.000,00
Standard Status Limit	0.90%	75,000
Excessive Status Limit	1.80%	250,000

Early Warning

Early warnings provide establishments with the opportunity to reduce fraud levels prior to entering the program. Visa sends monthly notifications to establishments that have not exceeded the program limits but have had 50,000.00 USD or more in reported fraud, and a fraud rate of 0.65% or more in the previous month.

Standard Status

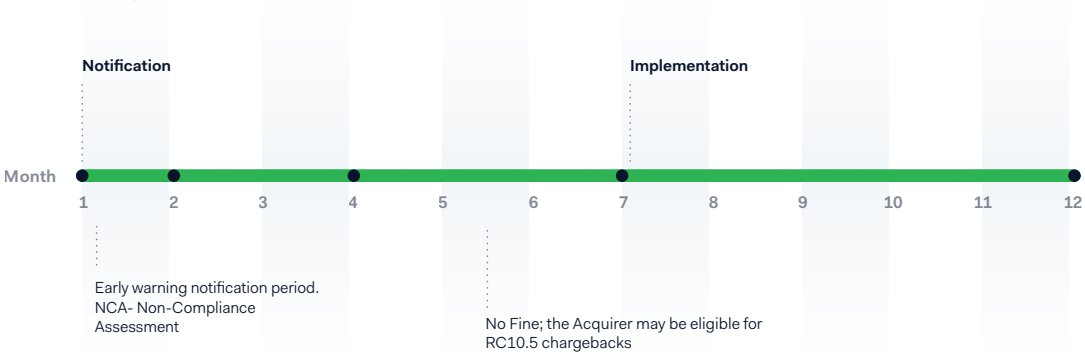
In the VFMP, an establishment enters the standard category if it meets or exceeds the following limits:

- ≥ 75,000 USD in reported fraud, and
- Fraud rate ≥ 0.9%

Deadlines and possible sanctions: upon exceeding the limits of the program, the establishment will have three months to comply with the rules without incurring penalties. Subsequently to month 4, however, the establishment qualifies for RC 10.5 Chargeback — Visa Fraud Monitoring Program. Under this chargeback motive code, it may lose the protection offered by 3D Secure — the issuer will have the right to chargeback using RC10.5, even if the transaction received may have its responsibility altered for 3D Secure authentication.

Figure 18

Deadlines and possible sanctions:



Excessive Status

An establishment will be assigned excessive status if it meets one of the following criteria:

1. high-risk MCC; or

The following MCCs are classified as high-risk:

- 5122 – Drugs, Drug Proprietors, and Druggists Sundries
- 5912 – Drug Stores, Pharmacies
- 5962 – Direct Marketing—Travel–Related Arrangement Services
- 5966 – Direct Marketing—Outbound Telemarketing Merchants
- 5967 – Direct Marketing—Inbound Telemarketing Merchants
- 7995 – Gambling Transactions

2. Exceed the excessive fraud rate and/or quantity limit; or

An establishment will enter the HR program if it meets or exceeds the following fraud limits:

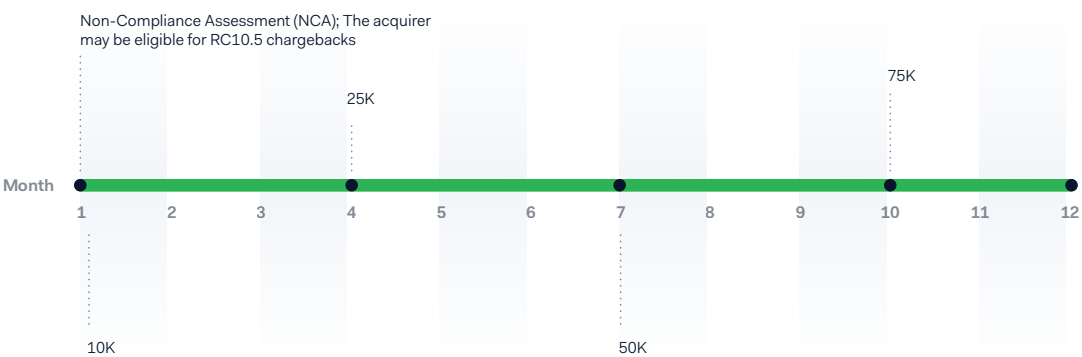
- ≥ 250,000 USD of reported fraud, and
- Fraud rate ≥ 1.8%

3. Establishments may enter the Excessive Status at Visa's discretion, based on a performance analysis (i.e. excessive fraud activity), misleading business practices, or potentially legal activities (such as Ponzi schemes).

Schedule and potential penalties: In the Excessive Status, there is no training period. Fines are imposed each month in which the establishment remains in the program. In addition, the establishment has the right to RC10.5 chargeback at the time it enters the VFMP with excessive fraud status.

Figure 19

Schedule and potential penalties



Note that RC 10.5 Chargebacks received as a result of VFMP identification do not count towards VDMP program calculations.

Correction/ Program Exit Criteria

In order exit the program, the establishment is required to maintain fraud levels below at least one of the standard status limits (75,000 USD fraud value and/or 0.9% fraud rate) for three consecutive months. If the establishment remains below the limits for two consecutive months, but exceeds them in the third month, the count will be reset and will not resume until the next month in which it shows results below the limits.

By continuing in the program for 12 months, either in the Standard or Excessive status, the establishment becomes subject to disqualification from the Visa payment system.

Figure 20

Standard Status examples

Reporting Month	FSR Ratio	Fraud Amount (USD)	Program Status	Penalty
June	0.98%	$ 130,000	Standard – Month 1	N/A
July	1.01%	$ 123,000	Standard – Month 2	N/A
August	0.87%	$ 105,000	Below average – Month 1 of 3	
September	0.85%	$ 107,000	Below average – Month 2 of 3	
October	0.95%	$ 119,000	Standard – Month 3	N/A
November	1.04%	$ 115,000	Standard – Month 4	N/A
December	0.93%	$ 124,000	Standard – Month 5	RC 10.5
January	0.89%	$ 108,000	Below average – Month 1 of 3	
February	0.70%	$ 99,000	Below average – Month 2 of 3	
March	0.52%	$ 80,000	Below average – Month 3 of 3	

Figure 21

Excessive Status examples

Reporting Month	FSR Ratio	Fraud Amount (USD)	Program Status	Penalty
June	1.75%	$ 160,000	Standard – Month 1	N/A
July	1.89%	$ 220,000	High Risk – Month 2	Applicable
August	1.85%	$180,000	High Risk – Month 3	Applicable
September	0.87%	$ 102,000	Below average – Month 1 of 3	
October	0.89%	$ 101,000	Below average – Month 2 of 3	
November	0.91%	$ 115,000	High Risk – Month 4	Applicable
December	1.02%	$ 124,000	High Risk – Month 5	Applicable
January	0.88%	$ 104,000	Below average – Month 1 of 3	
February	0.70%	$ 89,000	Below average – Month 2 of 3	
March	0.52%	$ 87,000	Below average – Month 3 of 3	

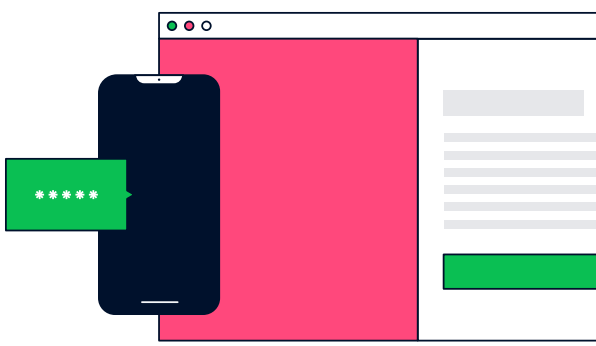
It is required to remain below the standard status limits for 3 consecutive months to exit the program.

The establishment exceeded the program's Standard Status and its limits for 2 months. To exit the program, the establishment must be below the Standard Status for 3 consecutive months.

Programas VFMP – VFMP–3D Secure (VFMP–3DS) – United States only

The VFMP-3D Secure program applies only to establishments using acquiring in the United States. The establishment enters the program if it exceeds the following fraud limits:

- ≥ 7,500.00 USD in reported 3DS fraud, and
- ≥ 0.75% 3DS FSR*



The program calculates the 3DS fraud sell rate (FSR) as follows:

Figure 22

January FSR Ratio

$$= \frac{\text{Total \$ amount of 3DS reported fraud in January}}{\text{Total \$ amount of 3DS sales in January}}$$

Early Warning

Early warnings provide establishments with the opportunity to reduce 3DS fraud levels before being identified in the VFMP-3DS. Visa sends monthly notifications for establishments that did not exceed the program limits but had 5,000.00 USD or more in reported fraud and 0.50% or more in 3DS FSR in the previous month.

Figure 23

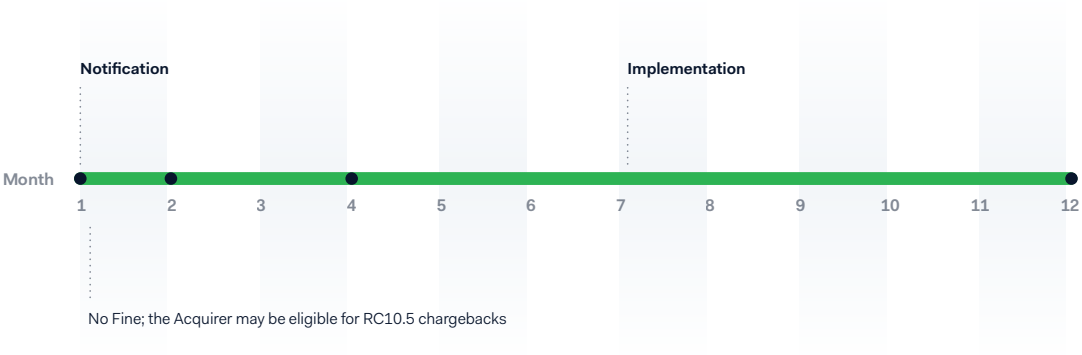
Early Warning and Standard Status Limits

	3DS Fraud Rate	Fraud Amount in Fraud
Early Warning Limit	0.50%	5,000 USD
Standard Status Limit	0.75%	7,500 USD

Deadlines and potential penalties: there are no fines associated with the VFMP-3DS program. However, once they are identified in the standard status, establishments immediately become liable for the chargebacks of the VISA RC10.5 Fraud Monitoring Program. Under this chargeback motive code, the establishment loses the protection offered by 3D Secure. Please note that RC10.5 chargebacks cannot be defended and automatically result in a chargeback loss.

Figure 24

Deadlines and potential penalties



Correction/ Program Exit Criteria

To exit the program, the establishment must keep 3DS fraud levels below at least one of the program's standard fraud limits (7,500 USD in 3DS and/or 3DS-FSR fraud amount at 0.75%) for 3 consecutive months. If this occurs for two months, and in the third it exceeds the limits again, the count will be reset. After 12 months in the program, the establishment may be disqualified from the Visa payment system.

ELO

No chargeback program in place. There are no fines in case of excess.

Amex

No chargeback program in place. There are no fines in case of excess.

About Adyen

Adyen is the payment platform chosen by leading global companies, offering a modern and complete infrastructure directly connected to VISA, Mastercard and other major payment methods. Adyen offers uncomplicated payments on online, mobile and in-store channels. With offices worldwide, Adyen works with 9 out of 10 of the largest online companies in the world. Its clients include Facebook, Uber, Netflix, iFood, GOL Linhas Aéreas, Rappi and Tok&Stock.

For more information, visit adyen.com