SHIFT4™

Fraud and Chargebacks Policy

Version 2.8 | January 2025

Contents

Introduction

This document contains the applicable fraud and chargeback thresholds for transactions deposited by Merchants and Payment Facilitators[1] ("PFs") acquired by Shift4.

In order to protect merchants/PFs and the payment ecosystem against excessive fraud and chargebacks, Shift4 is applying fraud and chargeback management programs. The programs are based on incremental thresholds to allow merchants/PFs to identify, contain and protect against fraudulent transactions and chargebacks through different measures in a timely manner. The tables below reflect Shift4's current risk appetite and are in line with the card scheme risk control programs.

Breaching any specific threshold Level outlined in this policy may lead to remedial action up to and including termination measures, if Shift4 is exposed to a substantial financial loss or reputational impact as may be determined by Shift4 in its discretion.

[1] Payment Facilitators are entities contracting and/or approving merchants on Shift4's behalf (referred to as sub-merchants). PF's are required to use a specific cardholder descriptor format: PF*merchant name. The aggregated volumes under such descriptor need to comply with the outlined thresholds. In addition, Shift4 expects the PF to manage the sub-merchants in line with the above thresholds and other card scheme rules.

Visa Acquirer Monitoring Program (VAMP)

Effective of 1 April 2025

The Visa VAMP program will replace all other Visa's fraud programs, including VFMP, VDMP and Digital Goods monitoring program.

Each month, Visa monitors card-absent domestic and cross border non-fraud disputes, fraud, and enumeration performance of Acquirers and their Merchants, based on the previous month's activities. Those who exceed the program identification thresholds as outlined in Visa VAMP Threshold Table are identified in the VAMP and responsible for taking appropriate actions and remediation.

VAMP Performance Definitions

Visa utilizes information from the following VisaNet transaction data to calculate the performance of VAMP metrics, included by not limited:

• All card-absent sales transactions submitted and processed through Visa in the previous calendar month by Central Processing Date (CPD). For example, sales transactions processed through Visa in March will be reported in April's VAMP Identification notification.

• Card-absent non-fraud disputes (dispute codes 11,12,13) submitted and processed through Visa in the previous calendar month by CPD.

• All card-absent fraud transactions (TC40) reported to Visa by issuers in the previous calendar month by fraud post-date.

• All card-absent Rapid Dispute Resolution (RDR) cases submitted and processed through Visa in the previous calendar month by CPD

VAMP Performance Metrics

The VAMP Ratio is calculated as follows:

$$\frac{Count\ of\ TC40\ +\ Non-Fraud\ Disputes\ -\ RDR\ cases)}{Count\ of\ Total\ Settled\ VISA\ Transactions}$$

There are two ways an Acquirer can be identified in the VAMP:

1. Acquirer exceeds the VAMP Ratio threshold as outlined in threshold table.

2. An Acquirer's merchant exceeds the VAMP Ratio threshold as outlined in threshold table.

Visa VAMP Threshold Table

Acquirer Portfolio			Merchant Portfolio				
Identification Level	**Above Standard**	**Excessive**	**Excessive**				
Data Elements	Vamp Ratio (bps)		Vamp Ratio (bps)				
Region	Global	Global	NA	EU	ASIAPAC	CEMEA	LAC
Threshold Effective Date April 1, 2025		>=50 bps	>=150 bps	>=150 bps	>=150 bps	>=150 bps	>=90bps
Threshold Effective Date January 1, 2026	>=30 to <50 bps	>=50 bps	>=90bps	>=90bps	>=90bps	>=150 bps	>=90bps

Additional Criteria

1. VisaNet transactions only, card-absent only, domestic and cross border
2. Minimum of 1,000 monthly combined fraud and non-fraud disputes excluding the RDR cases for merchant
3. Merchant Excessive Identification level applies only if Acquirer VAMP Ratio <30bps
4. Includes non-fraud dispute condition categories 11,12,13
5. Excludes Rapid Dispute Resolution (RDR) and Cardholder Dispute Resolution Network (CDRN)
6. Excludes confirmed Compelling Evidence 3.0 except for fraud disputes

VAMP Non-Compliance Assessments

Based on the following criteria, acquirers identified as Above Standard or Excessive in VAMP may be subject to enforcement actions, including the fees indicated in the table below, instead of non- compliance assessments.

If acquirer portfolio performance is above the specified threshold, enforcement fees will apply to each dispute (fraud and non-fraud) for all merchants with a VAMP ratio of >=30 bps.

If merchant performance is above the specified excessive threshold, enforcement fees will apply to each dispute (fraud and non-fraud) for that merchant only.

If an unsecured dispute fee is applied in the Europe market, the VAMP enforcement fee will not be applied to the same transaction.

Fees		
Acquirer Portfolio		Merchant
Above Standard	Excessive	Excessive
USD 5 per card-absent fraud and dispute non-fraud	USD 10 per card-absent fraud and dispute non-fraud	USD 10 per card-absent fraud and dispute non-fraud

Fraud Programs

Visa Fraud Monitoring Program (VFMP)

Valid until 31 March 2025

Visa Fraud Threshold Table

All frauds, first 10 reported for fraud Visa rule applies[2].

All fraud transactions	Thresholds	Control measures
Approaching (Shift4 Internal Threshold only)	0.5% & $20,000	Internal Fraud Alert Stage. Further information on merchant fraud & chargeback tools. 3ds authentication strategy + business practices might be requested on a case-by-case basis
Early Warning	0.65% & $50,000	Visa Official Fraud Alert Stage Notification letter to request implementation of authentication[3] + an action plan might be required
Standard	0.9% & $75,000	Visa Official Fraud Alert Stage. All the above + Action Plans and Visa Status are tracked and counted until merchant performs under the Standard threshold for 3 consecutive months. Scheme fees and reviewed reserves apply[4].
Excessive	1.8% & $250,000	Visa Official Fraud Alert Stage. All the above measures + control measures might be mandated or enforced, including termination & listing on VMAS.

Visa Fraud Rate Calculation Methodology

The fraud ratio is calculated at the beginning of each month for the previous month, i.e. the month in which all fraud has been reported by Card Issuers worldwide (the "Fraud Reporting Month").

The fraud ratio equals the total fraud value received during the Fraud Reporting Month / divided by the value of all transactions for that same reporting month per unique merchant descriptor.

For example: The March fraud ratio is calculated by dividing the fraud amount received in March by the total transaction value for March. The assessment is done the beginning of April.

Timelines

[2] Only the first 10 reported as a fraud transaction by same card to the same merchant account in the same calendar month are taken into consideration for the fraud ratio calculation.
[3] The merchant has to demonstrate adequate authentication mechanisms have been put into place or commit to implementation of same within a specific timeline.
[4] For Merchants trading under MCC codes (4816, 5122, 5816, 5912, 5966, 5967, 5968, 5993, 6012 – crypto, 6051 – crypto, 6211, 7273, 7995) a High Risk Assessment Timeline applies

When a merchant enters a program, they will only move through the program timeline for every month that they meet or exceed the program threshold. If the merchant is below the threshold, they do not move to the next step in the timeline. The merchant will proceed through the program timeline for each month in which it is identified in VFMP, until the required remediation period is met.

Standard Timeline

In the Standard timeline, merchants identified by the VFMP would be provided with one month of notification and three months of workout to reduce fraud levels. The three workout months do not have to be consecutive calendar months.

Enforcement Period	Months above Thresholds	Assessment	Notes
Notification	1	No Non-Compliance Assessment	---
Workout	2 -4		
Enforcement	5 -6	USD 25,000	Visa may allow issuers to raise fraud disputes on 3D Secure authenticated transactions
	7 -9	USD 50,000	
	8 -9	USD 50,000	
	10 -12	USD 75,000	

High Risk & Excessive Timelines

The High Risk & Excessive timeline does not have a workout period, only enforcement. Merchants qualify for the High-Risk timeline if they belong to or should belong to a High-Integrity Risk MCC or Merchants determined by Visa as causing undue harm to the goodwill of the Visa payment system may be accelerated to High-Risk status.

These merchants will remain in the High Risk or Excessive timeline for all future identifications until they complete their remediation by being below the Standard program threshold(s) for three consecutive months.

Enforcement Period	Months above Thresholds	Assessment	Notes
Enforcement	1 - 3	USD 10,000	Visa may allow issuers to raise fraud disputes on 3D Secure authenticated transactions
	4 -6	USD 25,000	
	7 - 9	USD 50,000	
	10 -12	USD 75,000	

Visa's Digital Goods Fraud Monitoring Program (MCCs: 5735, 5815, 5816, 5817, 5818)

Valid until 31 March 2025

All fraud transactions	Thresholds	Control measures
Approaching (Shif4 Internal Threshold only)	0.3% & 100 Fraud counts & $10,000 Fraud dollar amount	Internal Fraud Alert Stage. Further information on merchant fraud & chargeback tools. 3ds authentication strategy + business practices might be requested on a case-by-case basis
Early Warning	0.45% & 150 Fraud counts & $15,000 Fraud dollar amount	Visa Official Fraud Alert Stage Notification letter to request implementation of authentication[5] + an action plan might be required
Standard	0.9% & 300 Fraud counts & $25,000 Fraud dollar amount	Visa Official Fraud Alert Stage. All the above + Action Plans and Visa Status are tracked and counted until merchant performs under the Standard threshold for 3 consecutive months. Scheme fees and reviewed reserves apply[6].

Timeline

Merchants identified by the VFMP Digital Goods would be provided with one month of notification and three months of workout to reduce fraud levels. The three workout months do not have to be consecutive calendar months.

When a merchant enters a program, they will only move through the program timeline for every month that they meet or exceed the program threshold. If the merchant is below the threshold, they do not move to the next step in the timeline. The merchant will proceed through the program timeline for each month in which it is identified in the program, until the required remediation period is met.

Enforcement Period	Months above Thresholds	Assessment	Notes
Notification	1	No Non-Compliance Assessment	---
Workout	2 - 4		
Enforcement	5 -6	USD 25,000	Visa may allow issuers to raise fraud disputes on
	7 - 9	USD 50,000	

[5] The merchant has to demonstrate adequate authentication mechanisms have been put into place or commit to implementation of same within a specific timeline.

6 For Merchants trading under MCC codes (4816, 5122, 5816, 5912, 5966, 5967, 5968, 5993, 6012 – crypto, 6051 – crypto, 6211, 7273, 7995) a High Risk Assessment Timeline applies

Enforcement Period	Months above Thresholds	Assessment	Notes
	10 - 12	USD 75,000	3D Secure authenticated transactions

Mastercard Fraud Management Programs

Mastercard Fraud Program

Mastercard has postponed the launch date of its fraud program to a future date, yet to be announced. Future charges will be made upon previous notice.

To promote reduction of fraud levels across the industry, Mastercard has put in place fraud management requirements. Industry players that do not comply with these standards will face higher fees and fines.

To support these requirements, Shif4 has set its own Fraud Management program as described below:

1. The program is applicable for merchants located in the following countries: Andorra, Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Greenland, Hungary, Iceland, Ireland, Italy, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, Monaco, Netherlands, Norway, Poland, Portugal, Romania, San Marino, Slovakia, Slovenia, Spain, Sweden, Switzerland, Vatican City.[7]
1. Merchants are required to keep their fraud rates under 0.10%.
2. The calculation of the fraud rate includes all Mastercard domestic and intra-regional purchase transactions. The calculation is based on the following formula:
3. $Fraud\ rate = \frac{Total\ amount\ of\ fraudulent\ intra\ and\ domestic\ Mastercard\ transactions}{Total\ amount\ of\ intra\ and\ domestic\ Mastercard\ purchase\ transactions}$
4. The fraud rate is assessed monthly, three full months after the end of the assessed month. This ensures that most of the fraud notifications for the assessed month were already received, and the calculation is accurate (for example for transactions processed in February the fraud rate will be calculated during the month of June, and fees, if applicable will be charged accordingly).
5. Merchants who exceed the 0.10% fraud rate will be charged a fee according to the table below. The fee is a percentage of your total processed amount of domestic and intra-regional Mastercard purchase transactions:

Fraud tier	Min fraud rate	Max fraud rate	Fee
Tier 1	0.10%	0.50%	0.015%
Tier 2	0.50%	0.75%	0.030%
Tier 3	0.75%	1.00%	0.075%
Tier 4	1.00%	2.00%	0.100%

[7] The program will become effective in Switzerland and Liechtenstein as of 1 April 2024.

Fraud tier	Min fraud rate	Max fraud rate	Fee
Tier 5	2.00%	and up	0.150%

6. The program applies to all e-commerce transactions (card-not-present), it is calculated monthly, and only for merchants that had more than 1,000 transactions in the respective month.

Mastercard Excessive Fraud Merchant Program (EFM)

For merchant NOT incorporated in Andorra, Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Greenland, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Monaco, Netherlands, Norway, Poland, Portugal, Romania, San Marino, Slovakia, Slovenia, Spain, Sweden, Vatican City, the old Mastercard Excessive Fraud Merchant Program thresholds apply:

All fraud transactions	Threshold Regulated[8] Market	Threshold Non-Regulated Market	Control measure
Approaching (Shif4 Internal Threshold only)	1000 trn count $40,000 Fraud[9] CBK 0.40% Fraud CBK % 3DS % < than 50%	1000 trn count $40,000 Fraud - CBK 0.40% Fraud CBK % 3DS % < than 10%	Internal Fraud Alert Stage Further information on merchant fraud & chargeback tools in place and business practices might be requested on a case by case basis
EFM	1000 trn count $50,000 Fraud CBK 0.50% Fraud CBK % 3DS % < than 50%	1000 trn count $50,000 Fraud CBK 0.50% Fraud CBK % 3DS % < than 10%	Mastercard Official Fraud Alert Stage Notification letter to request implementation of authentication + an action plan required

Merchants in the following countries are excluded from the EFM Program:

- Liechtenstein
- Switzerland

Mastercard Fraud Chargeback Calculation Methodology

Shif4 applies the following methodology to calculate fraud chargebacks on cards issued globally:

- The chargeback ratio is calculated at the beginning of each month.

[8] The term regulated refers to those countries with a legal or regulatory requirement for SCA. (EU/EEA, Malaysia, Singapore, Nigeria)
[9] Monthly fraud-related chargebacks are defined as those chargebacks processed within a calendar month under either of the following reason codes:
• 4837 (No Cardholder Authorization)
• 4863 (Cardholder Does Not Recognize-Potential Fraud)

- The chargeback ratio equals the total chargeback count received during the previous month / divided by the total transaction count of the sales reference month.

For example: The February chargeback ratio is calculated by dividing the chargeback count received in February by the total transaction count for January. The assessment will be done the beginning of March.

Timeline

When a merchant enters a program, they will only move through the program timeline for every month that they meet or exceed the program threshold. If the merchant is below the threshold, they do not move to the next step in the timeline. The merchant will proceed through the program timeline for each month in which they are identified in the program, until the required remediation period is met.

Months above Thresholds	Assessment
1	No Non-Compliance Assessment
2	USD 500
3	UDS 1,000
4 -6	USD 5,000
7 - 11	USD 25,000
12 - 18	USD 50,000
19+	USD 100,000

Disputes Programs

Visa Disputes Monitoring Program (VDMP)

Valid until 31 March 2025

Visa Disputes[10] Threshold Table

All disputes, first 10 disputes Visa rule applies[11]

All chargebacks	Threshold	Control measure
Approaching (Shif4 Internal Threshold only)	0.50% & 50 Disputes	Internal Disputes Alert Stage. Further information on merchant fraud & chargeback tools in place and business practices might be requested on a case by case basis
Early Warning	0.65% & 75 Disputes	Visa Official Disputes Alert Stage. Notification letter to request implementation of authentication + an action plan might be required
Standard	0.90% & 100 Disputes	Visa Official Disputes Alert Stage. All the above measures + control measures might be mandated or enforced. Action Plans and Visa Status are tracked and counted until merchant performs under the Standard threshold for 3 consecutive months. Scheme fees and reviewed reserves may apply[12]
Excessive	1.8% & 1000 Disputes	Visa Official Disputes Alert Stage. All the above measures + control measures might be mandated or enforced, including termination & listing on VMSS Scheme fees and reviewed reserves apply

Visa Disputes Rate Calculation Methodology

To calculate disputes on cards issued globally, Shif4 applies the following methodology:

The dispute ratio is calculated at the beginning of each month. The disputes ratio equals the total disputes count received during the previous month / divided by the total transaction count of the previous month.

For example: The January chargeback ratio is calculated by dividing the chargeback count received in January by the total transaction count for January. The assessment will be done the beginning of February.

[10] 1st Chargeback
[11] Only the first 10 disputes by same card posted within same month on same merchant account are taken into consideration for the Disputes ratio calculation
[12] For merchants trading under MCC codes (4816, 5122, 5816, 5912, 5966, 5967, 5968, 5993, 6012 – crypto, 6051 – crypto, 6211, 7273, 7995) a High Risk Assessment Timeline applies

Timelines

When a merchant enters a program, they will only move through the program timeline for every month that they meet or exceed the program threshold. If the merchant is below the threshold, they do not move to the next step in the timeline. The merchant will proceed through the program timeline for each month in which it is identified in the program, until the required remediation period is met.

Standard Timeline

In the Standard timeline, merchants identified by the VDMP would be provided with one month of notification and three months of workout to reduce dispute levels. The three workout months do not have to be consecutive calendar months.

Enforcement Period	Months above Thresholds	Assessment
Notification	1	No Non-Compliance Assessment
Workout	2 -4	
Enforcement	5 -9	USD 50 per dispute
	10 -12	USD 50 per dispute and USD 25,000 review fee

High Risk & Excessive Timelines

The High Risk & Excessive timelines does not have a workout period, only enforcement. Merchants qualify for the High-Risk timeline if they belong to or should belong to a High-Integrity Risk MCC or Merchants determined by Visa as causing undue harm to the goodwill of the Visa payment system may be accelerated to High-Risk status.

These merchants will remain in the High Risk or Excessive timeline for all future identifications until they complete their remediation by being below the Standard program threshold(s) for three consecutive months.

Enforcement Period	Months above Thresholds	Assessment
Enforcement	1 - 6	USD 50 per dispute
	7 -12	USD 50 per dispute and USD 25,000 review fee

Mastercard Excessive Chargeback Program (ECP)

Mastercard Chargeback Threshold Table

All Chargebacks	Threshold	Control measure
Approaching (Former Internal Threshold only)	0.75% & 75 chargebacks	Internal Chargeback Alert Stage Notification letter
ECM - Excessive Chargeback Merchant	1.5% & 100 chargebacks	Mastercard Official Chargeback Alert Stage All the above measures + Revise reserves A 2nd month of breach may lead to termination. Scheme fines may apply
HECM - High Excessive Chargeback Merchant	3.0% & 300 chargebacks	Mastercard Official Chargeback Alert Stage All the above measures + Revise reserves. A 2nd month of breach may lead to termination. Scheme fines may apply

Mastercard Chargeback Rate Calculation Methodology

The chargeback ratio is calculated at the beginning of each month. The chargebacks ratio equals the total chargeback count received during the previous month/divided by the total transaction count of the month prior.

For example: The April chargeback ratio is calculated by dividing the chargeback count received in April by the total transaction count for March. The assessment will be done the beginning of May.

Timeline

Merchants will remain in the Excessive or High Excessive timeline for all future identifications until they complete their remediation by being below the threshold(s) for three consecutive months. *(Table appears in the next page).*

Months above Thresholds	ECM	HECM	Issuer Recovery Assessment
1	0	0	No
2	EUR/USD 1,000	EUR/USD 1,000	No
3	EUR/USD 1,000	EUR/USD 2,000	No
4 -6	EUR/USD 5,000	EUR/USD 10,000	Mastercard will charge €5/$5 for every chargeback over the first 300 chargebacks. *e.g.: A merchant with 1000 chargebacks doesn't pay for the first 300, and pays $3500 for the rest (1000-300 = 700, 700*5=3500)*
7 - 11	EUR/USD 25,000	EUR/USD 50,000	
12 -18	EUR/USD 50,000	EUR/USD 100,000	
19+	EUR/USD 100,000	EUR/USD 200,000	

Version Control

Version	Approval	Date	Description	Author
2.7	SVP Risk	March 2024	Postpone of Mastercard Fraud Program to an unknown effective date.	PMK Team
2.6	SVP Risk	November 2023	Rebranded to Shift4 Added the following MCCs to the VFMP and VDMP: 6012, 6211, 5968.	PMK Team
2.5	SVP Risk	October 2023	Added new effective date for VFMP digital goods and Mastercard fraud program.	Risk Team
2.4	SVP Risk	September 2023	Added Visa's Digital Goods program to VFMP. Added enforcement timelines to all programs.	Risk Team
2.3	SVP Risk	January 2023	Updated Mastercard fraud program starting date to April 2023 Updated the Mastercard fraud program thresholds EFM Program decommission for the countries starting the new program Expansion of Visa VDMP and VFMP to include domestic transaction as well	PMK Team
2.2	SVP Risk	May 2022	Added countries to the list of the program by Mastercard mandate. Changed the start date of the program. Excluded inter.	PMK Team
2.1	SVP Risk	March 2022	Updated the effective date of the new Mastercard program Added additional countries the program now applies in.	PMK Team
2.0	SVP Risk	February 2022	Update with Mastercard new Fraud Program	Fraud Team
1.2	SVP Risk	October 2019	Visa's updated fraud program	Fraud Team
1.1	SVP Risk	2017	Revision of Mastercard and Visa thresholds	Fraud Team
1.0	SVP Risk	2015	First Release	Fraud Team

Need Support?

Contact our Client Relations Centre 24/7 for any additional information or technical issue:

EU: +356 2778 0876

UK: +44.20.3608.1288

US: +1.617.715.1977

Email: support-europe@shift4.com