

Genome card processing requirements

Version 1.0 | Effective Date: August 2026

Introduction

The aim of this document is to clearly outline the rules, obligations, and financial liabilities you must meet to accept card payments safely and compliantly. Please review these requirements carefully, as they form a binding part of your contract with Genome. Failure to adhere to them may result in contract termination.

1. Pre-launch merchant checklist

To ensure a smooth launch and strict compliance, please ensure all the following requirements are met on your website before initiating live card processing:

- **Mandatory authentication (3DS):** The Payment Services Directive requires Strong Customer Authentication (SCA) for all electronic payments within the EEA. All payments, regardless of the amount, must be authenticated via 3D Secure (3DS).
- **Company information:** Clearly display your legal name, registered office address, permanent headquarters address, registered company number, and contact email/telephone number.
- **Policies and terms:** Publish your Terms and Conditions of Sale, a Consumer Data Privacy Policy, and a Shipping Policy (detailing delivery methods, timing,

and export restrictions).

- **Refund/return acceptance:** Publish a Company Policy covering refunds, returns, and cancellations that requires the Cardholder's explicit acceptance (e.g., a "Click to accept" button) at checkout.
- **Security disclosure:** Clearly state on your website how you keep customer payment data safe during checkout. You can do this by adding a brief sentence mentioning that you use secure, encrypted connections (like SSL) and do not store sensitive card details.
- **Clear offerings:** Ensure accurate descriptions, pricing, and transaction currencies are displayed for all goods/ services on the payment page.
- **Brand logos:** Display Visa and Mastercard logos strictly according to their official brand guidelines (unmodified and undistorted).
- **Technical Readiness:** Ensure you are fully enrolled in 3D Secure and comply with PCI DSS requirements applicable to your type of integration.

2. Core processing rules

- Mandatory authentication (3DS):** The Payment Services Directive requires Strong Customer Authentication (SCA) for all electronic payments within the EEA. All payments, regardless of the amount, must be authenticated via 3D Secure (3DS). You must enroll with Mastercard Identity Check if you would like to accept e-commerce Maestro (please contact us for more information).
- No unknown amounts:** Genome does not allow Merchant-Initiated Transactions (MIT) Mandates where the final amount is unknown at the time of authentication. You must confirm the exact gross amount prior to taking payment.
- Business classification:** You operate under a specific Merchant Classification Code (MCC). Please agree upon a new processing arrangement with us before diversifying or changing the goods/services you sell.
- Transaction classification:** You must strictly differentiate and flag Account Funding Transactions (AFTs) (e.g., wallet top-ups, account loads, funding of gaming or trading accounts) from regular purchase Transactions via Genome's API, based on the transaction nature and your MCC.
- Mandatory data:** For AFTs and specific high-risk MCCs (4829, 6540, 6051, 6211, 7800-7802, 7994-7995, 9406), you must transmit expanded cardholder data via API. This includes the cardholder's first and last name, date of birth, full billing address (street, city, state/region, country, ZIP code), and any required recipient details. Failure to provide this expanded Cardholder Data or misclassification of an AFT will result in immediate Transaction declines.

3. Security and fraud prevention

As the card and cardholder cannot be verified at the time of the transaction, CNP transactions carry increased risks. There is no guarantee that the person undertaking the transaction is the genuine cardholder, which means you may be at risk of chargebacks from fraudulent transactions. There are several simple ways you can reduce the risks for your business.

DO	DON'T
Get the cardholder's full name, phone number, and address, including the postcode (as recorded by their card issuer). Note: If the delivery address is different, ensure that you also get the delivery address and the name of the person receiving the goods or services.	Allow a cardholder to collect goods in person that were purchased via a CNP transaction.
Make sure you get the card number, expiry date, and the card security code (CSC). Also known as: CVC or CVC2: card verification code; CW or CW2: card verification value; CWC: card verification value code; CCV: card code verification; V-code or V code: verification code SPC: signature panel code	
Before taking payment, make sure you confirm the gross amount inclusive of all costs (e.g., delivery, packaging, VAT, etc.).	
Record the customer reference number, if quoted – for a Visa transaction only.	

4. Reviewing suspicious activity

Please proactively monitor and review transactions matching these profiles.

Initiate additional checks in these circumstances:

- a. **Location mismatches:** Non-EEA-issued cards where the delivery address country differs from the IP address country.
- b. **Duplicate activity:** Multiple orders from the same customer (incl. delivery address) or duplicate purchases.
- c. **Card irregularities:** Sequential card numbers or multiple cards used for a single order.
- d. **High-risk goods:** Orders made up solely of goods which can be easily re-sold, or orders that seem unusual due to a particularly large volume or value.
- e. **Address issues:** Orders not going to the registered card billing address, or if the address is suspicious (e.g., has it been used by a different customer before?).
- f. **Suspicious customer behavior:** Does the customer lack details of their account or previous orders, admit to using a card on someone else's behalf, or sound like they are being prompted/using a script?
- g. **Fraud history:** Use chargeback data to flag names, addresses, and IP addresses that are potentially used by fraudsters.

5. Mandatory refusals

Always make sure that goods or services are sent/provided to the person named on the order; never release goods to anyone else (including delivery firms hired by the customer).

For Direct API (Host-to-Host) integrations, you shall:

- Refuse the order if postcode or CSC verification fails.
- If the card has an invalid expiry date, refuse new orders.

For Hosted Payment Page (HPP) integrations: Genome automatically performs these verifications on your behalf and will return a declined status for any failed checks.

If you are still unsure about a transaction, or you require further information about any of our fraud tools or the checks recommended by the card schemes, contact your account manager or support@genome.eu.

6. Authorization and fulfillment

You must authorize a transaction at the time of the purchase (either for the full amount or a pre-authorization for the exact anticipated value). Remember, authorization confirms the cardholder has sufficient funds and that the card has not been reported as lost or stolen at the time of the transaction. Authorization doesn't guarantee payment.

Shipping goods and providing services

Mastercard	Visa
The transaction amount must not exceed the authorised amount.	Authorization for a Visa transaction is valid if the amount is within 15% of the authorized amount. The additional 15% must only be to cover the cost of shipping.
The transaction date is the date goods or services are provided or shipped.	The transaction date is the date goods or services are provided or shipped.
You must obtain authorization for Mastercard transactions on the day the cardholder places the order. The transaction should be processed when the goods or services are ready to be delivered. If you do not ship goods within seven days, you must obtain a second authorization. Quote the original auth. code, and keep both for your records.	A Visa transaction can be authorized up to seven calendar days before the transaction date.

7. Recurring transactions

When carrying out a recurring transaction, a merchant must:

- Obtain prior permission (in writing or electronically) from the cardholder to periodically charge for recurring services; and
- Retain a copy of that permission for the duration of that recurring transaction and provide it to the Issuer upon the Issuer's request.
- Ensure transactions are not more than 365 days apart.

- d. Ensure the correct card expiry date is provided for each transaction.

When entering a Recurring Transaction Agreement, a merchant must:

- a. Obtain express consent from the cardholder at the point of checkout or sale; and
- b. Provide the cardholder with the following information when obtaining that consent:
 - The amount of the recurring transaction;
 - Whether the amount is fixed or variable;
 - The date of the recurring transaction;
 - Whether the date is fixed or variable; and
 - An agreed method of communication for all future cardholder correspondence.

8. Account updater service

When using the account updater service, the merchant must:

- a. Ensure they are registered by Genome for services with each card association.
- b. Pass card data or be integrated into the Customer Vault API.
- c. Update databases containing the account information within five working days of receiving results of the Account Updater service, so that the latest updates are used for the next billing run.
- d. Have ongoing communication with cardholders who have a card account number and expiry date on file, and where the customer has an active recurring billing or subscription service with the merchant.
- e. Remove account information from the database of any account if you receive 'Contact Cardholder' or 'Closed' responses from the Account Updater service.

Upon receipt of such responses, the merchant must:

- Disable the billing service for that account.
- Halt the pending shipment of goods.
- Contact the cardholder to request new card information to use.

9. Payouts service (Visa Direct OCT)

The Original Credit Transaction (OCT) is a VisaNet Transaction that can be used to send funds to an eligible Visa account. Merchants can use the OCT to enable Visa Direct services such as money transfers, funds disbursement, prepaid loads, and

credit card bill payments.

Visa Direct services are available to Genome merchants who are registered in the following countries:

Austria	Hungary	Poland
Belgium	Ireland	Portugal
Denmark	Italy	Spain
Estonia	Malta	Sweden
Finland	Netherlands	Switzerland
France	Norway	UK
Germany		

When the Original Credit Transactions are used, please ensure you comply with the following rules.

- a. **Velocity checks and monitoring:** Comply with any transaction limits, volume limits, and velocity checks established by Genome. Monitor for suspicious activity, such as single senders initiating transactions to multiple recipients or high OCT volumes followed by disputes.
- b. **KYC and sanctions compliance:** You are solely responsible for verifying the sender for KYC, AML, and sanctions enforcement. Screen senders/recipients against blocked lists (e.g., OFAC, UN), comply with PCI DSS, and perform a Modulus-10 check on payment credentials.
- c. **Domestic transfers:** For domestic programs, validate that both the sender's funding source and the recipient's account reside in the same country before initiating the OCT.
- d. **Customer disclosures and receipts:** Provide a clear, itemized confirmation of payment details before execution (including transfer amounts and all merchant-assessed fees/FX markups). Senders must explicitly agree to these fees. Receipts must include sender/recipient names, masked payment credentials, date/time, total paid, exchange rates, and a Sender Reference Number.
- e. **Terms and Conditions:** Your program must have specific Terms covering product descriptions, security, transparent fees, and dispute policies. Explicitly state that P2P money transfers cannot replace purchase transactions.

10. Refunds and dispute management

- a. **Processing returns:** Process refunds using the same card used for the original transaction. The refund must never exceed the original transaction amount, and it cannot be used to credit winnings from gaming.
- b. **Handling disputes:** Retain transaction receipts securely in strict accordance with PCI DSS for at least 7 years following the transaction date, and produce them upon demand.
- c. **Requests For Information (RFIs):** Reply to RFIs clearly and legibly by the quoted date with all supporting documentation (authorization codes, T&Cs, transaction dates). Failure to supply a legible copy within the stated timeframe (usually 14 days) will result in a chargeback.

11. Compliance

- a. **PCI DSS:** Compliance with the Payment Card Industry Data Security Standard (PCI DSS) is mandatory at all times. If you become non-compliant, notify support@genome.eu immediately. You will be recharged for any Card Scheme non-compliance fees, Sensitive Authentication Data (SAD) storage fines, and data breach penalties imposed on Genome due to your non-compliance. Additionally, failure to provide valid PCI DSS documentation upon request will result in the monthly PCI DSS non-compliance fee being automatically deducted from your merchant account.
- b. **AFT and data compliance liability:** Any fines, penalties, or integrity fees levied by the Card Schemes or Our Partner (the acquiring bank) due to your failure to properly classify AFTs or transmit the mandatory expanded cardholder data will be treated as financial liabilities under Merchant Terms and Conditions and are subject to immediate deduction from your settlement funds or rolling reserve.
- c. **Consumer protection laws:** Comply with Consumer Contracts Regulations (CCRs) and E-commerce Regulations (ECRs) by refunding customers within 14 days of cancellation, providing online cancellation options, prohibiting pre-ticked boxes for additional items, and displaying total pricing and digital content compatibility prior to the transaction.

12. Mandatory notifications

Keep Genome informed: Notify support@genome.eu immediately regarding:

- a. Changes to your website addresses or the number of sites you operate.
- b. Changes to the nature of your business, goods/services provided, or legal entity status.
- c. Changes to your terms of sale (delivery times, warranties, refund policies, deferred payments).
- d. Changes to contact numbers, bank account details, postal/email addresses, or company directors/partners.
- e. Any Insolvency Event, change of control, or the sale/disposal of any material part of your assets that may result in a material adverse change to your business.

In case of any inconsistencies or conflicts between these Genome Card Processing Requirements and the Merchant's Terms and Conditions, the latter must prevail.