worldpay

Merchant Risk Guide – Payrix 2025

Getting Started

This guide is intended to provide new Partners with an introductory overview of the process and requirements related to merchant monitoring. By providing you with this information, we aim to provide transparency in the processes and enable you to effectively communicate the requirements to your merchant(s).

Pre-requisites

New Partners should have received their Approval Terms and have completed the Implementation process. The Partner should be assigned a Partner Experience Partner who will be the primary contacts to lead them through risk processes.

We understand that there are nuisances and unique use cases for each Partner that may need to be discussed in more detail with the Risk Team. To help this conversation and share known risks and best practices amongst the teams, a 30-minute Risk Kick-Off* meeting will be offered to new Partners. This meeting is intended to introduce situations in which risk is engaged and help the partner reduce cases in which friction may be applied.

If an additional, more in-depth conversation is needed to ensure the Partner is comfortable and clear on the approach, it will be scheduled accordingly.

*Risk Kick-off meeting should introduce this information and then documentation that offers additional resources and one stop shop for onboarding information.

Merchant and Transaction Monitoring

Ongoing Monitoring

Payment processors use advanced algorithms and tools to monitor transactions for fraudulent activity, helping businesses minimize their exposure to fraud. Both transaction and merchant monitoring are Anti-money laundering/Combating the Financing of Terrorism (AML/CTF) Regulatory requirements for Payment Processors.

Merchant Monitoring

Merchant monitoring assesses risk at the merchant level rather than the transaction level. This solution helps to monitor merchants engaged in both low- and high-risk industries to help payment service providers avoid Mastercard Business Risk Assessment and Mitigation (BRAM) Program and the Visa Integrity Risk Program (VIRP) — formerly the Global Brand Protection Program (GBPP) fines. Merchant monitoring can help identify the risk that transaction monitoring would miss by reviewing merchant's websites and wider web presence.

Transaction Monitoring

Transaction monitoring is the process of identifying suspicious payment transactions, usually using a combination of technology and human review. Transaction monitoring is a part of compliance with due diligence requirements and is monitored at the transaction level to protect against money laundering and fraudulent activities.

Hold Transparency

From time to time, the Merchant or Transaction Risk teams will need to hold a transaction while mitigating the risk. The Portal offers insights into when transactions are under review by the Risk team in the Risk Section of the Portal.

In addition to the Risk section of the Portal, webhooks and email alerts can also provide insight into the transaction status. Webhooks can also be set up to notify your server when transactions are impacted by Risk Holds. Email alerts can be sent to partners and/or merchants when an action triggers an event.

Account Takeover (ATO)

Account Takeover is a form of credential theft because it involves the theft of login information, which then allows the criminal to steal for financial gain. When a processing account is taken over, the fraudster will make small, non-monetary changes to the account, which may include adding authorized user information, changing passwords, or adding financial information controlled by the fraudster.

Account Takeover Methods

There are several ways a bad actor can get the credentials needed for account takeover, in addition to data breaches or buying them on the dark web.

- Phishing
  - Phishing schemes, often conducted via email or text, are designed to get victims to provide account information to fraudsters. This type of social engineering is characterized by tricking victims by impersonating legitimate organizations, like government agencies and banks, or victims' family and friends. Victims who unknowingly fall for these types of fraud provide bad actors with easy access to their accounts.
- Phone Scams
  - This form of social engineering is perpetrated by scammers pretending to be tech support in need of access to the victim's computer or a grandchild who needs banking information to transfer funds for an emergency.

- Unsecure Wi-Fi
    - Personal Wi-Fi needs to be secure, which may require changes to default settings and passwords. Public Wi-Fi should never be used for anything important, especially when it involves logging into accounts. A bad actor can set up a man-in-the-middle attack by creating a fake wireless access point in a public location and use it to intercept your internet activity.
- Password Sharing
    - Login details may be compromised due to data breaches or leaked passwords from other websites. If you reuse passwords, attackers might try them on different platforms. Practice good password hygiene and monitor all accounts. Each account should have a unique password.
- Credential Stuffing / Password Cracking / Brute Force Attacks
    - Credential stuffing uses bots to test compromised credential combinations on multiple websites or apps to access accounts.
    - Password cracking tools automate the use of leaked or stolen usernames with dictionaries of common passwords, sometimes supplemented with custom dictionaries, to access accounts.
    - Brute force attacks are a popular cracking technique that involves trying different variations of symbols or words until the correct password is figured out.
- Session Hijacking
    - Authenticated user sessions are supported by storing a session and authentication token on the client device (e.g., cookie in the browser). Attackers may bypass the login and take over an account by stealing a valid token. Stealing a token may be done using different techniques such as Man-In-The-Middle (MITM), Man-In-The-Browser (MITB), and others.

Card Testing

Card testing is a type of fraudulent activity where someone tries to figure out whether stolen card information is valid so that they can use it to make purchases. A fraudster may do this by buying stolen credit card information, and then trying to confirm or make purchases with those cards to figure out which cards are still valid. Other common terms for card testing are “carding”, “account testing”, and “card checking.”

Card testing has many negative outcomes, some of which get worse over time as card testing continues:

- Disputes
    - Many types of card testing involve payments, some of which succeed. Customers notice successful payments and report them as fraud, which will result in disputes.
- Higher decline rates
    - Card testing usually causes many declines to be associated with your business. A high decline rate damages the reputation of the business with card issuers and card networks, which makes all transactions appear riskier. This can result in an increased decline rate for legitimate payments, even after card testing stops.
- Additional fees
    - Card testing activity can result in additional fees, such as authorization and dispute fees.

Buyer Fraud

All businesses, whether the business is for goods or services, online or in-person, are susceptible to buyer fraud. In its simplest terms, buyer fraud is the intentional targeting of a business by a fraudulent buyer who:

- does not intend to make or honor payment for goods or services (i.e., buyer abuse) OR
- does not intend to pay for goods or services with funds they are authorized to use (i.e., bad buyer)

Buyer fraud commonly results in disputed payments (e.g., unauthorized, not as described, and/or non-receipt claims). Disputed payments can be detrimental to a business because the merchant may end up liable for these payments resulting in losses and other potential impacts to the bottom line. While disputed transactions are unavoidable, there are steps that merchants can take to help protect themselves when experiencing disputed payments.

Buyer abuse can be very difficult to identify and address prior to a payment being processed. Merchants are best equipped to implement security measures that will set them up to be able to successfully refute a dispute. The following should be considered:

- Proof of shipping/delivery confirmation.
- Strong record keeping.

Bad buyer (or true fraud) activity often will have indicators that merchants can be vigilant for to minimize the potential impacts these transactions could have on their business. Merchants should consider the following:

- Authorization procedures. “Decline” codes passed by financial issuer should be honored by a merchant as this can be an indicator from the financial issuer of risk or potential other concerns that they are aware of. Do not re-attempt or repeat the transaction when a “decline” is received, simply ask for an alternate form of payment.
- Card not present (CNP) controls. This type of payment is prone to higher risk. Therefore, merchants should leverage Address Verification Service (AVS), CVV/CVC2 security features, and employ strategies to know their customer.
- Know your customer (KYC). These standards are designed to protect against fraud through strategies meant to help verify customer identities. This can be done by collecting and retaining buyer contact details associated with a payment including making photocopies of valid IDs.
- Be vigilant. Don’t be afraid to question whether something that seems out of the ordinary is a red flag, for example questions like:
    - Is this buyer attempting to make multiple payments using multiple financial instruments with several various addresses? If so, can this be reasonably justified by the buyer and is the justification practical?
    - Is this person attempting to make a payment using a financial instrument they claim to belong to someone else without that person present?
    - Through the details provided by the buyer match security services or features like AVS and CVV/CVC2?

Bad Merchants

Although we are constantly evolving and improving our detection strategies to make sure we are onboarding legitimate merchants who intend to use their processing account for approved transacting. On a rare occasion a bad actor may circumvent our onboarding checks, or a good merchant may go bad, we are obligated to mitigate the financial loss exposure and the regulatory risk.

Mitigating the Risk

Transaction Specific Risks

Transaction Monitoring has several distinct actions depending on the level of mitigation:

- Block
  - A block will prevent certain actions from occurring. A block could stop transactions from processing, funds from exiting, or prevent all transactional activity on the merchant account. A block is typically placed when the activity is believed to be too risky to continue or requires additional verification before it can continue.
- Hold
  - A hold will be used when a transaction requires a manual review. This can occur if the transaction amount exceeds the amount that was previously approved during onboarding or if the account experiencing unusual or unexpected activity.
- Reserve
  - A reserve is used as a safeguard to prevent unplanned chargebacks or returns. When there is a reserve on an account, the merchant can continue to transact but will not have access to the funds in the reserve until the risk of chargeback or return has passed.

Although a transaction may be held or in reserve, that does not always mean that documentation is needed to release the transaction. The Merchant and Transaction Risk teams will review the account and activity to decide if outreach to the partner is necessary. If more details are needed, the team will contact the Partner to request the necessary information to clear the transaction and release the hold/reserve.

On occasion, the transaction reserve or hold, or account hold may remain in place while the investigation continues as not all risk can be mitigated with documentation.

Merchant Related Risks

If, during the review of the merchant's account, it is determined that the merchant is responsible for the increased risk on the account, mitigation will be required. Mitigation actions will be applied to address the risk presented.

- Disbursement Block
  - A disbursement block is applied when an investigation is required to make sure funds leaving the Payrix system are processed legitimately, and the risk of return is nominal.
- Refund Block
  - A refund block may be applied when a merchant is processing excessive refunds or refunds are causing the processing account to go negative and there is a risk that the funds will not be recovered from the merchant’s bank account.
- Transaction Block
  - Transactions may be blocked for several reasons – to prevent ongoing card testing or to stop a merchant from processing additional transactions while an investigation is ongoing.
- Delayed Funding
  - Funding delays may be applied if there is a reason to suspect that a merchant poses an increased credit risk and will not be able to offset Returns or Disputes. This may

be the result of past recovery rejects, excessive disputes, or a vertical with a high dispute or return rate.

Documentation Overview

This guidance will provide clarification on the types of documentation needed to mitigate risks found on merchant accounts or associated with a specific transaction. In these situations, more documentation may be requested. The following list is not an exhaustive list but should be considered guidance.

Business Documentation

Type of Risk	Documentation Accepted
Transaction Risk	• Transaction details with buyer contact information: Invoice, Contract, Work Order, etc. • Identification Information: State Issued identification or Passport • Confirmation that buyer has funds available to avoid return: i.e., Bank Guarantee
Credit Risk	• Transaction details with buyer contact information: Invoice, Contract, Work Order, etc. • Merchant financial liquidity to offset chargebacks, returns, disputes: Cash Flow statements, Bank Account Statements, etc. • Supplier documentation and/or proof of ability to fulfill order • Proof of shipping/delivery • Processing History
Merchant Fraud Risk	• Transaction details with buyer contact information: Invoice, Contract, Work Order, Shipping/Delivery Details, etc. • Business Information: Articles of Incorporation, Business license, Secretary of State certification, etc. • Identification Information: State Issued identification or Passport • Explanation requested: Merchant Controls in place, reason for payment, etc. • Processing History
AML (Anti Money Laundering) Risk	• Business details, which could include AML programs, licenses, 3rd Party verification services, etc.
Reputation Risk	• Transaction details with buyer contact information: Invoice, Contract, Work Order, etc. • Supplier details

Documentation Review

Once documents are provided, they will be reviewed by the Analyst. Their review will ensure that the documents are not altered or falsified and provide the necessary information to mitigate the risk identified. On occasion, the documentation provided may not mitigate the risk or result in additional requests.

Helpful Resource Center Articles

Transaction Risk – Best Practices

Transaction Risk Prevention

- Risk Strategies
- Transaction Risk Documentation

Merchant Risk Prevention

- Risky Merchants OnePagers

Account Takeover Best Practices

Mitigate Card Testing Attacks

Understanding Risk Types

Setting up Webhooks

Setting up Email Alerts