

VALMAR

The holiday readiness guide

Protect your payments, prevent fraud, and keep
businesses moving this holiday season.



BEFORE THE RUSH

Is your business holiday-ready?

The holiday season can be one of the most profitable times of the year for businesses. It can also be one of the most challenging.

Higher transaction volumes, larger purchases, new customers, and increased fraud attempts can put additional pressure on your payment processing setup.

And when business is booming, the last thing you want is an unexpected payment hold, a surge in chargebacks, or a technical issue slowing down checkout.

The good news? A little preparation can go a long way.

Whether you operate a retail store, e-commerce business, restaurant, or service-based company, taking time to review your payment operations before the holiday rush can help you avoid unnecessary disruptions.

This guide covers five essential payment checks, three common holiday fraud tactics, and a simple action plan to help your business stay prepared.

INSIDE THIS GUIDE

- 01 Your 5-point holiday payments check
- 02 Holiday fraud watch
- 03 Your holiday payments action plan
- 04 What to do when something goes wrong
- 05 Growth, not payment problems

01

CHECK 1 OF 5

Review your processing limits

More sales are great. Unexpected payment interruptions aren't.

During the holidays, many businesses experience significant increases in transaction volume. While this is good for revenue, unusual activity can sometimes trigger additional reviews by payment processors or acquiring banks.

Merchant accounts may have established processing parameters, including monthly transaction volume and maximum individual ticket amounts.

If your holiday sales exceed your normal activity, it's important to communicate those expectations ahead of time.

YOUR ACTION PLAN

Review last year's holiday sales, estimate this year's expected volume, and contact your payment processing representative before major promotions begin.

If you're expecting substantial growth, ask whether your current processing parameters are appropriate.

WHAT TO CHECK

- ☐ **Monthly processing volume:** How much do you typically process each month, and how much do you expect during the holidays?
- ☐ **Maximum transaction size:** Will holiday purchases, bulk orders, or gift card sales increase your average ticket?
- ☐ **Sales patterns:** Are you planning promotions, flash sales, or seasonal campaigns that could create sudden transaction spikes?
- ☐ **New products or services:** Are you introducing anything that could change your account's processing profile?

VALMAR TIP

Don't wait until your busiest sales day to discuss an increase in volume. Proactive communication gives your processing team time to review your account and address potential issues.

02

CHECK 2 OF 5

Make sure customers recognize your business on their statements

An unfamiliar charge can quickly become a disputed charge.

Your billing descriptor is the name that appears on a customer's bank or credit card statement after they make a purchase.

If that name doesn't match the business they remember purchasing from, they may assume the transaction is fraudulent.

For example, a customer might shop at a store called "Main Street Boutique" but see a charge from an unfamiliar parent company or legal business name.

Even when the transaction is legitimate, that confusion can lead to unnecessary disputes.

YOUR ACTION PLAN

Make a test purchase and review how the transaction appears on a card statement once it posts.

If the descriptor is confusing, ask your processor what changes are possible. Descriptor formatting and length may be subject to card network and processor requirements.

WHAT TO CHECK

- ☐ Does your billing descriptor closely match your customer-facing business name?
- ☐ Would a first-time customer recognize it?
- ☐ If you operate multiple brands, is the descriptor clear?
- ☐ Is your customer service contact information easy to locate?

VALMAR TIP

Include your recognizable business name and customer service information in order confirmations and receipts. The easier you make it for customers to identify a purchase, the less likely they are to dispute it out of confusion.

03

CHECK 3 OF 5

Review your refund and return policies

Clear expectations can prevent expensive misunderstandings.

Holiday shopping often comes with more returns, exchanges, shipping delays, and customer service questions.

When customers don't understand how to request a refund, they may contact their bank instead of contacting your business. That can turn a manageable customer service issue into a payment dispute.

A transparent, easy-to-find return policy helps customers understand their options before making a purchase.

YOUR ACTION PLAN

Review your current policy and make sure it's easy to understand.

Consider creating a dedicated holiday returns section that addresses extended return windows, final-sale items, shipping timelines, and refund processing expectations.

Place links to your policy in prominent locations, including your checkout page, confirmation emails, and customer support section.

WHAT TO CHECK

- ☐ Is your refund and return policy clearly visible on your website?
- ☐ Are customers informed of important terms before checkout?
- ☐ Do receipts and confirmation emails reference your policy?
- ☐ Are holiday return deadlines and exceptions clearly explained?
- ☐ Does your team understand how to handle refund requests?

VALMAR TIP

Make it easier for customers to resolve issues directly with you than through their bank. Responsive customer service and transparent policies are valuable tools for reducing avoidable disputes.

04

CHECK 4 OF 5

Review your chargeback alerts and fraud prevention tools

The earlier you identify a problem, the more options you may have to address it.

Chargebacks occur when customers dispute transactions through their card issuers.

During the holiday season, disputes may increase due to higher transaction volumes, delivery issues, customer confusion, or fraudulent purchases. Even legitimate transactions can be disputed, and responding requires time and documentation.

The right alerts and monitoring tools can help your business identify suspicious activity and respond to eligible disputes sooner.

YOUR ACTION PLAN

Contact your payment processing representative to review which fraud prevention and dispute management tools are available for your account.

If early dispute alerts are supported, ask how they work and what actions your business can take when one is received.

Keep in mind that not every alert prevents a chargeback, and some programs have specific response windows or fees.

WHAT TO CHECK

- ☐ Are chargeback notifications being delivered to the correct person?
- ☐ Does your payment setup support early dispute alerts?
- ☐ Are you monitoring unusual transaction activity?
- ☐ Does your team know how to respond to a chargeback?
- ☐ Are transaction records, receipts, and delivery confirmations easily accessible?

VALMAR TIP

Keep organized transaction records throughout the holiday season. When a dispute occurs, having documentation readily available can make the response process much easier.

05

CHECK 5 OF 5

Update your business contact information

When something needs attention, being reachable matters.

Payment processors and their banking partners monitor transaction activity to help identify potential fraud and account risk.

If your business experiences an unusual sales spike or suspicious transaction pattern, your processing team may need additional information.

Outdated contact information can delay important conversations and make resolving issues more difficult.

YOUR ACTION PLAN

Confirm your contact information with your processor before the holiday rush.

If your business will operate with reduced staff or modified hours, designate someone who can respond to urgent payment-related inquiries.

WHAT TO CHECK

- ☐ Is your primary business phone number current?
- ☐ Are your account email addresses actively monitored?
- ☐ Do you have a backup contact for urgent matters?
- ☐ Will the right person be available during holiday closures?
- ☐ Does your team know whom to contact if a payment issue arises?

VALMAR TIP

Save your payment processing support information somewhere your team can easily access it. A clear escalation plan can save valuable time when problems arise.

PART 2 · HOLIDAY FRAUD WATCH

3 common fraud tactics every business should know

Holiday shopping brings increased sales opportunities, but it also creates opportunities for fraudsters.

Higher transaction volumes can make suspicious activity harder to spot, especially when teams are busy fulfilling orders and serving customers.

Understanding common fraud tactics is the first step toward protecting your business.

TACTIC 01

Card testing

TACTIC 02

Friendly fraud

TACTIC 03

Account takeover

FRAUD TACTIC 01

Card testing

WHAT IS IT?

Card testing happens when criminals use stolen card information to attempt transactions, often through automated bots. They may submit numerous small purchases or authorization attempts to determine which stolen cards are still active.

These attempts can create unnecessary processing costs, increase declines, and expose your business to additional fraud risk.

WARNING SIGNS

- A sudden spike in small-dollar transactions
- Multiple declined transactions in a short period
- Repeated attempts from the same IP address or device
- Numerous payment attempts using different card numbers
- Unusual checkout activity outside normal business hours

HOW TO PROTECT YOUR BUSINESS

Use bot protection. CAPTCHA or other automated traffic detection tools can help reduce bot-driven checkout activity.

Set transaction velocity controls. Limit repeated payment attempts within a short period when supported by your gateway.

Review security settings. Consider available tools such as address verification (AVS), card verification (CVV), and fraud screening.

Monitor declines. A sudden increase in failed transactions can be an early warning sign.

TAKEAWAY

A large number of failed transactions isn't always harmless. Investigating unusual patterns early can help prevent larger problems.

FRAUD TACTIC 02

Friendly fraud

WHAT IS IT?

Friendly fraud occurs when a legitimate cardholder disputes a transaction they actually authorized.

Sometimes these disputes are intentional. Other times, they result from confusion, forgotten purchases, unrecognized billing descriptors, or dissatisfaction with an order.

For example, a customer may receive an item but claim it never arrived, or forget about a purchase and report the charge as unauthorized.

WARNING SIGNS

- Customers repeatedly disputing completed purchases
- Claims of non-delivery despite tracking confirmations
- Disputes involving clearly documented transactions
- Customers contacting their bank without first contacting your business

HOW TO PROTECT YOUR BUSINESS

Use recognizable billing descriptors. Help customers identify legitimate purchases.

Keep thorough records. Save receipts, order confirmations, delivery tracking, and relevant customer communications.

Communicate proactively. Notify customers of shipping delays, backorders, and changes to fulfillment timelines.

Make support accessible. Provide clear contact information and a straightforward refund process.

TAKEAWAY

Strong documentation and clear customer communication can help prevent unnecessary disputes and support your response when one occurs.

FRAUD TACTIC 03

Account takeover

WHAT IS IT?

Account takeover occurs when a criminal gains unauthorized access to a legitimate customer's online account. Using stolen login credentials, fraudsters may change account details, update shipping addresses, or place unauthorized orders.

Because the activity originates from an existing customer account, it can sometimes appear legitimate.

WARNING SIGNS

- Sudden changes to shipping addresses or contact details
- Logins from unfamiliar devices or locations
- Multiple failed login attempts
- High-value purchases shortly after account changes
- Unusual urgency around order fulfillment

HOW TO PROTECT YOUR BUSINESS

Encourage strong authentication. Use multifactor authentication where available.

Verify sensitive changes. Require additional confirmation before changing important account information.

Monitor unusual activity. Review orders that involve unfamiliar devices, significant account changes, or atypical purchasing behavior.

Train your team. Make sure employees know when to flag suspicious orders for additional review.

TAKEAWAY

A familiar customer account doesn't automatically mean a transaction is safe. Changes in behavior can be just as important as changes in payment details.

WHAT TO DO BEFORE THE RUSH

Your holiday payments readiness checklist

You don't need to overhaul your entire payment operation to prepare for the holidays. Start with the areas most likely to affect your ability to accept payments and serve customers. Use this checklist to make sure you've covered the essentials.

PROCESSING & ACCOUNT SETUP

- ☐ Review expected holiday transaction volume.
- ☐ Confirm monthly processing and maximum ticket parameters.
- ☐ Notify your processor about anticipated sales spikes.
- ☐ Review any new products, promotions, or changes in business activity.

CUSTOMER EXPERIENCE & DISPUTE PREVENTION

- ☐ Verify your billing descriptor.
- ☐ Review refund, return, and cancellation policies.
- ☐ Confirm that customers receive clear order confirmations.
- ☐ Make customer support information easy to find.
- ☐ Establish a process for handling customer complaints quickly.

FRAUD & SECURITY

- ☐ Review available fraud detection settings.
- ☐ Enable applicable transaction and dispute alerts.
- ☐ Check bot protection and transaction velocity controls.
- ☐ Train employees to recognize suspicious activity.
- ☐ Confirm that transaction and delivery records are retained securely.

COMMUNICATION & SUPPORT

- ☐ Update primary and backup business contacts.
- ☐ Confirm holiday support procedures.
- ☐ Identify who will monitor payment activity.
- ☐ Make sure employees know how to report suspicious transactions.
- ☐ Save your processor's support contact information.

PART 4

What to do when something goes wrong

Even well-prepared businesses can encounter payment issues during the holidays. What matters is recognizing problems quickly and knowing how to respond.

IF YOU NOTICE**A sudden increase in declined transactions**

Check for unusual patterns, such as repeated attempts from the same device or IP address.

Review your fraud settings and contact your payment processing provider if the activity appears suspicious.

IF**A customer disputes a transaction**

Review the reason for the dispute and gather relevant documentation, including receipts, delivery confirmations, and customer communications.

Follow the instructions and deadlines provided through your dispute management process.

Avoid issuing a separate refund without first confirming the appropriate next step, as doing so could create a duplicate credit.

IF**Your sales exceed expectations**

Contact your payment processing representative as soon as possible to discuss the increase.

Be prepared to share information about promotions, transaction volume, and any changes to your business activity.

IF YOU**Suspect fraudulent activity**

Document what you're seeing and contact your payment provider or risk team promptly.

If you suspect a customer account has been compromised, follow your established security procedures and protect the affected account.

REMEMBER

Early communication can make payment-related issues easier to investigate and resolve.

 PART 5

Make this holiday season about growth, not payment problems

The holidays should be an opportunity to grow your business, build customer relationships, and finish the year strong. Your payment processing setup should support that growth, not create additional obstacles.

By reviewing your processing parameters, strengthening fraud prevention, improving customer communication, and keeping your account information current, you can reduce avoidable risks and enter the holiday season with greater confidence.

And you don't have to navigate everything on your own.

YOUR PAYMENT PARTNER

Your business deserves a payment partner that's there when you need one

At Valmar, we understand that reliable payment processing is essential to keeping your business moving.

Our team brings hands-on underwriting and risk expertise, flexible payment solutions, and real human support to help businesses navigate the complexities of accepting payments.

Whether you're anticipating higher transaction volumes, reviewing fraud prevention options, or simply want to make sure your account is ready for the season, we're here to help.

Get ahead of the holiday rush.

Contact your Valmar representative to review your payment setup, discuss potential risks, and prepare for the busy season.

[TALK TO THE TEAM →](#)

VALMAR · YOUR TRUSTED PAYMENTS PARTNER

Disclaimer: This guide provides general educational information and is not a guarantee against fraud, chargebacks, processing interruptions, or account holds. Available fraud tools, processing parameters, and dispute procedures vary by merchant account, payment gateway, and banking partner. Contact your Valmar representative for guidance specific to your business.