atb.com

ATB MERCHANT FRAUD DEFENCE GUIDE

Your Guide to Fighting Fraud*

This guide is designed to be a practical, actionable resource to help you protect your business. We have broken down fraud prevention into a series of parts, from understanding the current risks to implementing technical controls. Use these sections to train your staff, strengthen your procedures, and build a resilient defense against fraud.

Navigating this Guide

- **Part 1: Why This Matters Now** Explains the shift to card-not-present (CNP) fraud and introduces the three essential tools, Address Verification Service (AVS), Card Verification Value (CVV), and EMV 3-D Secure, that form the foundation of your defense.
- **Part 2: Spot the Risk by Channel** Provides detailed checklists for identifying suspicious behavior and high-risk patterns, with specific guidance for both in-person (card-present) and online/phone (card-not-present) sales.
- **Part 3: The Essentials to Do Every Time** Outlines the core habits that should be part of every transaction, including the correct use of chip and PIN, signature verification, and secure refund procedures.
- **Part 4: Refunds and Chargebacks** Details the best practices for processing refunds to prevent fraud and provides a step-by-step guide on how to build a strong evidence-based case when responding to chargebacks in Moneris Merchant Direct.
- **Part 5: Protect Your Devices** Focuses on the physical security of your point-of-sale (POS) terminals, covering daily tamper checks, access control, and the steps to take if a device is compromised or stolen.
- **Part 6: When to Pause or Refuse** Offers clear guidance and professional scripts for safely pausing or refusing a transaction when something feels wrong, ensuring fairness for customers and safety for your team.
- **Part 7: Activating Tools** Provides a technical overview of how to enable and configure key anti-fraud tools within your Moneris setup, including AVS, CVV, EMV 3-D Secure, and real-time screening services like Kount Essential.
- **Part 8: If You Suspect Fraud** Lays out an immediate action plan for what to do the moment you suspect fraud, including how to use a Code 10 authorization call and what information to document for an incident report.
- **Part 9: Review Your Limits** Explains the importance of setting and regularly reviewing your transaction limits, velocity rules, and other controls to ensure they align with your business's sales patterns and risk tolerance.

Each section builds on the last, giving you a complete playbook for fraud prevention. Let's begin with Part 1 to understand why these steps are so critical right now.

Part 1: Why Fraud Prevention Matters

Card-not-present (CNP) fraud has become the biggest risk facing Alberta merchants today. As more in-person payments move to chip and tap, it's gotten harder for criminals to use stolen or counterfeit cards at the counter. But fraud hasn't disappeared, it's just shifted to remote channels like phone orders and online checkouts, where it's much tougher to know who's really on the other end.

Why is this happening?

With chip technology, called EMV, short for Europay, Mastercard, and Visa, every in-person payment is protected by a unique one-time code, making stolen card data nearly impossible to reuse. Fraudsters go where security is weakest, so when your customer isn't standing in front of you, it's easier for them to use stolen information or fake an identity.

What does this mean for your business?

Whenever you accept a card-not-present payment, you're taking on more risk. If a real cardholder later disputes a charge, your business could be responsible for the loss. That's why having a clear, consistent process isn't just best practice, it's your frontline defense. It helps you stop fraudulent orders before they go through, and it gives you the proof you'll need if a chargeback comes your way.

Three Practical Shifts to Make Now

1. Focus on the highest-risk areas

Start by strengthening your website checkout and any mail or phone order (also called MOTO, Mail Order/Telephone Order) processes. Use Address Verification Service (AVS) and Card Verification Value (CVV) checks for every CNP transaction. Set up your payment system to automatically decline mismatches, or flag them for your review before fulfilling the order.

2. Add stronger authentication for online sales

Turn on EMV 3-D Secure for your e-commerce payments. This tool lets the cardholder's bank run invisible risk checks in the background. If anything looks suspicious, the customer is asked to prove their identity, often with a one-time passcode or a fingerprint.

EMV 3-D Secure can reduce unauthorized purchases and, in many cases, shift fraud liability away from your business.

3. Watch for signs and respond quickly

Fraudsters often test stolen cards in batches. Keep an eye on your Moneris Merchant Direct reports for patterns like bursts of small, unusual charges, multiple declines, or lots of different cards tried on the same order. Acting fast can help you block a flood of fraud and prevent a wave of chargebacks later.

Set Your Team Up for Success

Fraud prevention works best when everyone follows the same playbook. Train your staff to use these tools and to stick to your verification process every time. Make sure your checkout and point-of-sale systems are set to record all AVS, CVV, and EMV 3-D Secure results, along with customer communications and delivery proof. If a chargeback happens, this documentation will be your best defense.

The Bottom Line

Fraudsters are always looking for the soft spot. Right now, card-not-present payments are the main target. By using the right tools, authenticating buyers carefully, and following a consistent review process, you can protect your business from losses, and put yourself in a strong position if a dispute comes up down the road.

Part 2: Spot the Risk by Channel

Knowing the unique risks in each sales channel helps your team act with confidence and consistency. Use the checklists below to train new staff, refresh experienced team members, and strengthen your online review process, without making things harder for good customers.

In Person (Card-Present): What to Watch For and What to Do

Recognizing suspicious behaviour

- A customer gathers expensive items quickly, barely comparing or asking questions.
- A shopper seems rushed, avoids eye contact, or tries to distract your team at the till.
- A card comes from a pocket, not a wallet, or the name on the card does not match how the customer introduces themselves.
- Someone insists on manual key entry, asks you to swipe a chip card, or wants to "try another card" after a decline.
- Multiple cards are used to split one purchase, especially for gift cards or items that are easy to resell.

Essential card checks every time

- Always insert the chip and ask for a Personal Identification Number (PIN), or use tap when possible. Only swipe if the terminal asks after a failed chip read.
- Check the card's security features and expiry date. If the card needs a signature, compare the one on the receipt to the card.
- If a card is unsigned, have the customer sign it in front of you and show government-issued photo identification. If they refuse, pause the sale.
- Never skip PIN entry unless the terminal prompts for a signature. Never accept "verbal authorization" from anyone claiming to be the bank.
- Avoid manual key entry. If you must key a card due to a damaged chip, get extra verification (such as photo identification) and make detailed notes on the receipt.

When to pause or refuse a sale

- If something feels wrong, stop and ask a supervisor for support.

- Use a “Code 10” authorization call if you suspect fraud in person. This process quietly alerts the card issuer while you answer simple yes-or-no questions.
- Politely refuse a sale if a customer insists on risky workarounds, such as manual entry for a chip card, refunding to a different card, or splitting payment across several cards without explanation.

Online or Phone (Card-Not-Present): Signs a Transaction Deserves a Closer Look

High-risk order patterns

- Unusually large or first-time orders that don’t match your typical sales, especially for goods that are easy to resell.
- Rush or overnight shipping for expensive items, paired with pressure to ship right away.
- Billing and shipping details that do not match, such as different names, distant provinces, or international shipping when your business usually ships locally.
- Many cards used the same address, phone number, or Internet Protocol (IP) address in a short time.
- Email addresses that do not match the buyer’s name, use throwaway domains, or are random strings of letters and numbers.
- Repeated declines followed by one approval, or a cluster of tiny authorizations, classic signs of card testing.
- Use of freight forwarders, parcel lockers, or unverifiable commercial addresses, especially when you usually ship to homes.

Controls to enable and how to use them

- **Address Verification Service (AVS)** compares the street number and postal code from your customer with the records at their bank. Set your payment gateway to automatically decline AVS mismatches or flag them for manual review.
- **Card Verification Value (CVV)** is the three- or four-digit code on the card. Always require it for every online or mail order/telephone order (MOTO) transaction. Decline any CVV mismatch.
- **EMV 3-D Secure** (often called Visa Secure or Mastercard Identity Check) adds a step where the bank may challenge the buyer with a one-time passcode or fingerprint. When successful, this lowers fraud and can shift liability to the issuer.

- **Velocity limits** set a cap on the number of attempts from a single device, email, card, or IP address in a given time. This stops card testing before it drives up your fees and chargebacks.

Before you ship

- Hold and verify any order with multiple red flags. Call the customer using the number they gave you and ask neutral questions to confirm details.
- Look up the shipping address in a mapping tool, and for high-risk orders, ask the customer to reply from their email confirming the order, the delivery name, and address.
- Use secure payment links for phone sales instead of key-entering card numbers. If you do need to take card data by phone, document all verification steps in your order notes.
- Require a signature on delivery for high-value shipments, and keep tracking, delivery confirmation, and all customer communication with the order record.

Quick Reference: When in Doubt

- **In person,** use a Code 10 authorization and bring in a supervisor.
- **For online or phone sales,** hold the order, run AVS and CVV checks, consider EMV 3-D Secure, and verify the details directly with the customer before shipping.
- **Always document your steps.** Consistent notes and saved results from AVS, CVV, and EMV 3-D Secure are your best defense if a payment is ever disputed.

Part 3: The Essentials to Do Every Time

These habits apply to every sale, every day. Build them into your team's training, point-of-sale routines, and e-commerce settings so that safe payments are the default.

Chip with Personal Identification Number (PIN) or contactless tap, every time you can

- **Why it matters:** Chip and tap transactions create a unique code for each sale. This makes it much harder for anyone to copy or counterfeit card data, which protects your business from fraud and unnecessary disputes.
- **How to do it:** Insert the card and have the customer enter their PIN, or use contactless tap for payments within the allowed limit. Only swipe if the terminal asks you to after the chip has failed.
- **What to avoid:** Never bypass PIN entry unless the terminal asks for a signature. Do not force a magnetic stripe swipe on a chip card. If the chip is damaged, ask for a different payment method.

Compare signatures when prompted

- **When to check signatures:** You will still see signature prompts if a chip card falls back to a magnetic stripe, or if you are processing some international cards.
- **How to do it right:** Compare the signature on the receipt with the signature on the back of the card. If the card is unsigned, ask the customer to sign it in front of you and show government-issued photo identification. If they refuse, pause the sale and ask a supervisor for help.

Never refund to a different card or payment method

- **Why it matters:** Refund abuse is a common way criminals turn stolen purchases into untraceable cash or value. Refunding the original payment method protects you and ties the credit back to the real sale.
- **How to do it:** Start every refund from the original transaction in your point-of-sale system. Manager approval is needed for higher amounts. Always make a note of the approval in your records.
- **If you cannot refund the original card:** If the original card issuer declines the refund, follow your store's written policy. Offer store credit or refund to the same payment method when possible, not to a different card brand or cash.

Avoid key-entered card numbers from phone or email whenever possible

- **Why it matters:** Keyed-in card numbers miss out on chip security, and they are at much higher risk for fraud and chargebacks. Card numbers taken by phone or email are just as risky.
- **Safer alternatives:** Use secure payment links or direct your customer to your online checkout, instead of accepting card numbers over the phone. If you have to use a virtual terminal, go further, verify the customer's details with Address Verification Service (AVS) and Card Verification Value (CVV), call them back at a trusted number, and add detailed order notes.
- **If you truly must key a card:** Collect extra documentation, like a signed order confirmation and photo identification if the order is picked up in store. Ship only to addresses you have verified and require a signature on delivery.

Your One-Minute Checklist at the Till or Checkout

- ☐ Chip with PIN or tap used, never forced swipe on a chip card.
- ☐ If prompted for a signature, compare it to the card and check the ID if unsigned.
- ☐ Refunds always processed to the original transaction and method, with manager approval recorded when needed.
- ☐ No key-entered card unless absolutely necessary. If keyed, add extra verification and notes.
- ☐ For every card-not-present order, required AVS and CVV. Reviewed or declined any mismatches.

Documentation to Save with Every Sale

- Authorization response and amount
- AVS and CVV results for card-not-present payments
- Any 3-D Secure authentication data for online orders
- Order communications, ID check for pickup, shipment tracking, and delivery signature where used
- Manager approvals for refunds or overrides

Making these steps second nature keeps your business strong, helps your team work with confidence, and gives you the best protection if a payment is ever questioned down the road.

Part 4: Refunds and Chargebacks

Refunds and chargebacks impact your cash flow, your team's time, and your customer relationships. The right policy, strong controls, and fast follow-up in Moneris Merchant Direct help protect your business and keep trust strong.

What "good" refunds look like

- **Tie every refund to the original sale:** Use your payment terminal or online gateway to look up the original transaction and start the refund from there. This links the credit directly to the sale, helps prevent refund fraud, and keeps your records clean.
- **Refund only to the original method:** If a customer paid by credit card, return the funds to that exact card. Never refund to a different card brand, cash, or a gift card. If the original card issuer declines the refund, follow your written exception policy and record the reason for your files.
- **Require manager approval for larger refunds:** Pick a threshold that fits your business, such as the top five percent of your usual ticket size. Require a manager code or a second set of credentials for these refunds, and note the reason for the refund every time.
- **Reconcile refunds every day:** Run a daily refunds report in Merchant Direct. Make sure every refund ties back to an original sale and a return receipt or authorization. If something does not match, investigate before closing the batch.
- **Separate duties when you can:** If possible, the person who processes refunds should not be the one reconciling them. This simple check helps prevent internal fraud.
- **Publish and enforce a clear return policy:** State your return timeframes, condition-of-goods requirements, proof-of-purchase rules, refund method, restocking fees if any, and how customers can reach you. Share this policy at checkout, on receipts, and on your website.
- **Reduce "courtesy refunds":** Many chargebacks start as service frustrations. Give your team simple scripts and clear authority to solve problems without reflexively refunding. Offer exchanges or repairs where you can, and document what was done to resolve the issue.

Chargeback 101

A chargeback happens when a cardholder asks their bank to reverse a payment. Common reasons include “fraudulent or unauthorized,” “merchandise not received,” “not as described,” or “processing error.” In card-not-present sales such as phone or e-commerce orders, merchants carry more liability if identity was not properly verified.

- **Timelines are tight:** Moneris Merchant Direct shows the response deadline for each case. Aim to respond within one business day. Missing the deadline usually means losing the dispute automatically.
- **Evidence is everything:** Submit clear, relevant documents that match the reason for the chargeback. Avoid sending unrelated files. Write a short cover note that connects your evidence to the issue for the reviewer.

How to respond well in Merchant Direct

1. **Open the case the day you receive it:** Check the reason code and deadline. Assign a staff member to handle it, and set a reminder before the cutoff.
2. **Build the right evidence pack:** Match your evidence to the reason code. For example:
    - If the chargeback is for **fraud or unauthorized use** on a card-not-present order, include AVS and CVV results, any EMV 3-D Secure authentication data, the order date and time, IP address and device info if you have them, the invoice, all customer messages, and proof of delivery with a signature for high-value orders.
    - If the claim is **“merchandise not received,”** submit carrier details, tracking history, delivery confirmation, signature on delivery if you collected it, pickup log with photo ID for in-store pickup, and any customer messages confirming receipt.
    - If it is **“not as described” or “defective,”** include your product description, photos, service notes, correspondence offering to repair or replace, and your return policy as shown at purchase.
    - For **“processing error” or “duplicate,”** attach original authorization and capture logs, any void or reversal receipts, and the final receipt with the corrected amount.
3. **Write a short cover note:** Summarize your position in three to five lines. Clearly state what happened, why the charge is valid, and direct the reviewer to your attached evidence by name. Keep your explanation neutral and factual.

4. **Submit and track:** Upload your evidence in Merchant Direct. Make sure the case status updates. Calendar a follow-up date. If you lose the case, note the reason and update your process to avoid similar issues in the future.

When to fight and when to accept

- **Fight chargebacks when your evidence is strong:** If your records are solid and you followed policy, respond. Winning chargebacks deters future abuse.
- **Accept when evidence is weak:** If you cannot prove delivery, cardholder identity, or participation, accepting the loss prevents wasted time and keeps your dispute ratio in check.

One-Page Refund Checklist for Your Team

- ☐ Find the original sale and start the refund from that transaction.
- ☐ Refund only to the original method and card.
- ☐ Get manager approval for refunds over your set limit and record the reason.
- ☐ Match the refund to inventory or service records and reconcile the same day.
- ☐ Record any exceptions and keep documents with your daily batch.

Chargeback Response Checklist

- ☐ Open the case in Merchant Direct and note the deadline.
- ☐ Confirm the reason code and select the right evidence.
- ☐ Include AVS, CVV, and EMV 3-D Secure results for card-not-present orders.
- ☐ Add delivery proof, customer communications, and return policy documentation.
- ☐ Write a short cover note and submit before the deadline.
- ☐ Review the outcome and update your process if needed.

A clear process for refunds and chargebacks not only protects your bottom line but also shows customers you care about getting it right. Acting quickly and documenting every step is your best strategy for keeping losses low and relationships strong.

Part 5: Protect your devices

Your point-of-sale (POS) terminals are more than just cash registers, they process payments, read cards, and help verify your customers' identity. If a terminal is stolen, swapped, or tampered with, you risk financial loss and the exposure of your customers' card data. Treat every terminal like cash: limit who can access it, keep it in sight, and check it every day.

What good device security looks like every day

- Keep every terminal where staff can see it. Never leave a reader unattended on a self-serve counter unless there is a camera watching or the device is physically tethered.
- Perform a daily tamper check before opening and again at close. Log the results in a simple sheet and keep 90 days of logs on file.
- Match every device's serial number to your master inventory. If the serial number does not match, stop and investigate.
- Require manager credentials for refunds, voids, and admin functions. Cashier roles should be limited to sales only.
- Change all default passwords on the first day. Rotate manager passcodes at least once every quarter and immediately whenever someone leaves your team.

Physical security that prevents tampering

- Lock or tether devices to the counter using a bolted stand or security cable. A locked mount stops someone from quickly swapping the device.
- Keep a current photo of each terminal model your store uses, including the keypad, ports, and back plate. Use these photos to spot overlays or changes.
- Control who can touch terminals. Only let designated staff or verified technicians handle them. Verify any visiting technician by calling the Moneris number on your sticker or your ATB support line. Do not rely on a business card alone.
- Store spare or mobile readers in a locked drawer or safe. Log every checkout and return by name and time.
- Place cameras so they cover each till and terminal. Try to keep at least 30 days of footage if possible.

Daily tamper check: 60 seconds per device

- Inspect the seams, screws, and card slot for glue, pry marks, or loose parts. Gently test the keypad or any overlay.
- Make sure the base, cables, and any pin pad are firmly attached. Watch for unfamiliar dongles, splitters, or wires.
- Power on and print a test receipt if your terminal allows it. Confirm that the merchant name and device ID look correct.
- Compare the serial number on the device label to your master list. Record the check in your log with initials and the time.
- If anything looks different from yesterday's log or photo, stop using the device and move to incident steps.

If a device goes missing or seems tampered with

- Power the device off. Disconnect it from power and the network, then place it in a sealed bag so any attached skimmer remains in place.
- Call ATB or Moneris right away at **1-866-433-5204** (prompt 1 for ATB, prompt 2 for Moneris, available 24 hours a day). Report the serial number and when you last checked the device.
- Review the last 48 hours of transactions in Merchant Direct for anything odd, like a wave of small authorizations or repeated declines.
- Pull the last "clean" photo or log entry for the device and save security footage covering the till for the last two days.
- Do not hand the device to anyone except a verified Moneris technician or law enforcement if instructed.

Quick reference for training cards

- ☐ Treat all terminals like cash, keep them locked down and never leave them unattended.
- ☐ Check every device for tampering at open and close, always match the serial number, and record every check.
- ☐ Restrict admin access, change default passwords, and rotate manager passcodes.
- ☐ If anything seems off, stop using the device and call **1-866-433-5204** for help right away.

Protecting your devices is about habits, not just hardware. Simple daily checks, secure handling, and clear logs keep your business, and your customers, safe.

Part 6: When to pause or refuse

Protecting your business sometimes means taking a step back or saying no. Let your team know it is always okay to pause a transaction, verify more details, or refuse to proceed when something does not feel right. Use neutral, professional language, follow the process below, and document your actions. The main goals are staff safety, fairness for every customer, and reducing the risk of fraud losses.

What is a pause versus a refusal?

- **A pause** is a temporary hold while you confirm more information. This could mean calling the card issuer, running Address Verification Service, confirming a shipping address, or asking for government-issued photo identification in store.
- **A refusal** is a decision not to complete the sale. Reasons might include failed verification, obvious signs of tampering or a counterfeit card, unsafe behaviour, or your business policy not allowing a certain method.

Clear triggers to pause or refuse

In person

- The customer insists you swipe or key-enter a chip card after the terminal prompts for a chip.
- A shopper rushes, distracts staff, or tries multiple cards for one purchase, especially for gift cards or high-resale items.
- The card has mismatched or missing security features, looks damaged, or the signature panel appears altered.
- A request to refund a different card or method than was originally used.
- The device looks different from your last tamper check, or the serial number does not match your log.

Online or phone (card not present)

- Unusually large first order, rush shipping, mismatched billing and shipping details, or delivery to a freight forwarder or parcel locker without a clear business reason.
- Multiple cards used to the same address, phone number, email, or Internet Protocol address in a short period.
- Address Verification Service or Card Verification Value fails, or EMV 3-D Secure authentication does not go through.

- Repeated small authorizations or many declines, a sign of card testing.

How to pause without escalating

In-person scripts

- *"Thank you. Our system needs a quick verification to protect cardholders. I am going to make a brief call and we will be right back on track."*
- *"I cannot swipe a chip card unless the terminal instructs me. Do you have another form of payment we can try?"*

Online or phone scripts

- *"Thanks for your order. Before we ship, we need to confirm a couple of details. Can you reply to this email with the name on the mailbox and a contact number we can reach right now?"*
- *"For security, we use Address Verification Service and Card Verification Value on all phone orders. The address or code did not match. We can either try again, or you can use our secure payment link."*

Using Code 10 authorization for in-person doubts

A Code 10 authorization is a discreet call to the card issuer if you suspect a fraudulent transaction at the counter. The operator will ask you simple yes-or-no questions and guide you on whether to proceed, decline, or retain the card (only if safe).

- **When to use Code 10:** If a card looks altered, the cardholder's behaviour is suspicious, or the terminal gives odd responses, step aside and make the call, do not alarm the customer.
- **How to start a Code 10 call:** From your till, call Moneris at **1–866-319-7450**. Clearly state that you need a Code 10 authorization and follow the instructions given.

A decision flow your team can follow

1. Something feels off, or a control fails.
2. Pause the transaction and explain you need to verify details.
3. For in-person sales, consider a Code 10 call. For online or phone orders, run AVS and CVV again, check EMV 3-D Secure status, and review for other risk signals.

4. If verification is successful, proceed and note what you checked. If verification fails or the risk stays high, refuse the transaction and offer an alternative, like in-store pickup with identification or a wire transfer for business customers.
5. Document what happened in your order or terminal notes.

What to record every time you pause or refuse

- Date, time, location, staff initials, and device identifier if in store.
- What triggered the pause, such as AVS or CVV mismatch, failed EMV 3-D Secure, or unusual behaviour.
- What you did next, such as Code 10 call, customer call-back, or email confirmation.
- Outcome, whether you proceeded, refused, or offered an alternative payment option.

Why this protects you

Short, neutral explanations and a consistent process make things easier for your staff, reduce confrontation, and give you a clear record of what happened. If a dispute ever becomes a chargeback, your AVS and CVV results, EMV 3-D Secure data, and internal notes show that you followed policy and acted in good faith to protect both your customer and your business.

Part 7: Activating tools

The quickest way to cut fraud and reduce chargebacks is by turning on the right controls in your Moneris setup. The essentials below work best as a team. Start by enabling Address Verification Service and Card Verification Value for every card-not-present order, add Europay, Mastercard, and Visa (EMV) 3-D Secure for e-commerce, and layer on real-time fraud screening to stop patterns like card testing.

Address Verification Service (AVS) and Card Verification Value (CVV) for Mail Order, Telephone Order (MOTO), and e-commerce

- **What these tools do:** Address Verification Service checks the numeric parts of the billing address the buyer provides against the card issuer's records. Card Verification Value is the three-digit code on the back of most cards or the four-digit code on the front of American Express. Requiring CVV helps confirm the shopper has the card in hand.
- **Why they matter:** AVS and CVV stop many stolen-card attempts before they happen, and they give you clear, objective data for any dispute. Good customers will barely notice, but you will benefit from stronger protection.
- **How to set up in Moneris Gateway or your virtual terminal:**
    1. Enable AVS and CVV on every card-not-present payment form, including phone orders in your virtual terminal.
    2. Set AVS to decline any clear mismatch, and only approve matches you are comfortable with.
    3. Set CVV to decline any code mismatch.
    4. Make sure AVS and CVV response codes are saved with every order and are easy to find in your reports.

Europay, Mastercard, and Visa (EMV) 3-D Secure for e-commerce

- **What this is:** EMV 3-D Secure adds a quick authentication step during online checkout. Most shoppers pass automatically through a background risk check, but higher-risk orders may prompt the customer to confirm their identity with a passcode or biometric using their own bank.
- **Why it matters:** EMV 3-D Secure reduces unauthorized use and, for eligible sales, can shift fraud liability to the card issuer. This means fewer losses and less work for you on disputed transactions.
- **How to enable and get started:**

1. Ask Moneris to turn on EMV 3-D Secure for your e-commerce gateway or plug-in.
2. Use risk-based authentication so low-risk shoppers enjoy a smooth experience and only higher-risk orders are challenged.
3. Add a simple message at checkout explaining that their bank may ask to confirm their identity.
4. Test the process with different card types before you launch, try domestic, business, and international cards.

Kount Essential or similar real-time fraud screening

- **What this is:** Kount Essential is an AI-driven tool available through Moneris that screens every transaction in real time. It analyzes device, network, behavioral, and history signals to assign a risk score, then applies your rules to approve, review, or decline orders.
- **Why it matters:** Fraud usually happens in bursts, like card testing or scripted attacks. Automated screening stops most fraud before it reaches your accounts or shipping room, while letting good orders through.
- **Quick-start rules that work for most merchants:**
  - **Velocity limits:** Cap how many attempts one card, email, device, or IP address can make (for example, no more than three tries in fifteen minutes).
  - **Small-amount clustering:** Decline or review when many authorizations are made for low dollar amounts in a short time.
  - **Address and identity mismatches:** Escalate any order where billing and shipping postal codes are far apart, or names do not match across fields.
  - **Disposable email filters:** Flag orders from disposable or random email domains for review.

Success checklist to confirm you are live

- ☐ Address Verification Service and Card Verification Value are enabled and enforced for every card-not-present payment.
- ☐ EMV 3-D Secure is active at checkout and authentication data is saved with the order.
- ☐ Kount Essential or an equivalent fraud screening tool is running with starter rules for velocity, clustering, and mismatches.
- ☐ Someone is assigned to manage the review queue, and a playbook is in place.

- [ ] Weekly reports show declines for mismatches and smoother approval flow for returning customers.

Turning on these tools makes fraud prevention part of your daily routine, helping protect your business, your customers, and your peace of mind.

Part 8: If you suspect fraud

When you spot something suspicious, acting fast is essential. Your first priority is to stop the loss. Your second priority is to document everything so you can respond to any disputes and prevent future issues. Follow these steps for both in-person and card-not-present scenarios, then complete the short incident record at the end.

What to do in the first 60 seconds

1. **Stop the transaction.** Do not complete the sale. If you are in the middle of processing, press cancel on the terminal. For online orders, move the transaction to manual review or on-hold status.
2. **Keep everyone safe.** Never accuse, detain, or escalate with a customer. If there is any threat of violence, end the interaction and call local police right away.
3. **Call for help.** From your till or office, call **1-866-433-5204** (prompt 1 for ATB, prompt 2 for Moneris, available 24/7).
4. **Decide on next steps.** For an in-person card that does not feel right, ask for a **Code 10 authorization** during the call. For an online or phone order, ask the agent to review the authorization and help you decide what to do before you ship.
5. **Preserve evidence.** Do not clear your terminal, receipt, or browser tab until you capture the authorization result, date, time, and device ID. For e-commerce, save the order screen and payment gateway log.
6. **Document the trigger.** Write down exactly what made you suspicious, like an AVS mismatch, CVV mismatch, failed EMV 3-D Secure authentication, unusual behavior, or device tampering.

In-person playbook

- If the card looks altered, the customer is rushing or distracting staff, or the terminal acts oddly, pause and step aside to call for a **Code 10 authorization**. The operator will guide you through simple yes-or-no questions and tell you whether to proceed, decline, or retain the card if safe.
- If instructed to keep the card and it is safe, place it in an envelope with the date, time, staff initials, and the last four digits. Keep it in a locked drawer for pickup. Never put staff at risk to retain a card.
- If you suspect device tampering, power the terminal off, unplug it, and place it in a sealed bag. Switch to a backup terminal if you have one, and call

1-866-433-5204. Save security camera footage for the last two days showing the till area.

Card-not-present playbook for online or phone orders

- Move the order to manual review and do not capture payment or ship until verified.
- Re-check **Address Verification Service (AVS)**. A mismatch is a red flag.
- Re-check **Card Verification Value (CVV)**. A mismatch is a red flag.
- Confirm **Europay, Mastercard, and Visa (EMV) 3-D Secure** status. If authentication failed or was not used, treat the order as high risk.
- Review payment logs and your fraud tool for patterns like repeated declines, many small authorizations, or multiple cards going to the same address or Internet Protocol (IP) address.
- Call the customer using the number on the order and ask neutral questions to confirm details. If the answers do not add up, cancel and refund the order.

The quick incident record your team must complete

- ☐ Date and time, staff initials, location, and device ID (if in store)
- ☐ Transaction amount, authorization code, and whether the sale was cancelled or declined
- ☐ Trigger for suspicion (e.g., AVS mismatch, CVV mismatch, failed EMV 3-D Secure, unusual behaviour, or device tampering)
- ☐ Actions taken (e.g., Code 10 authorization, call to 1-866-433-5204, manual review, or removing a device)
- ☐ Outcome (e.g., declined, cancelled, card retained, order refunded, or referred to police)
- ☐ Follow-up steps (e.g., reviewing nearby transactions in Merchant Direct, updating fraud rules, or additional team training)

Why this process protects you

You stop losses before they settle. You document the evidence you will need for a chargeback. You build a reliable record that helps you train your team, supports ATB and Moneris investigations, and lowers the risk of fraud happening again.

Part 9: Review your limits

Your payment limits and controls are like seatbelts for your business. If they are set too loose, you can get hit hard by fraud. Set them too tight, and you might block good customers from completing their purchase. A simple quarterly review with ATB and Moneris keeps your limits in step with your sales, seasonality, and risk comfort level.

What "limits" include and why they matter

- **Per-transaction ceilings:** The maximum amounts your system will approve for a single sale or refund.
- **Daily and weekly volume caps:** The total dollar value or total count of transactions allowed per day or week.
- **Velocity limits:** Rules that cap how many attempts can happen for each card, email, device, or IP address.
- **Manual key-entry permissions:** Defines when staff can key in a card number and how much is allowed.
- **Refund controls:** How much can be refunded at once and whether a manager code is needed.

How to set the right limits using your own data

1. **Pull the last 90 days of sales and refunds in Merchant Direct.** Look for your average ticket size, the 95th percentile ticket, and your highest sales day.
2. **Set your ceilings just above your normal peaks.** A good rule is to set your per-sale ceiling at your 95th percentile ticket plus a small buffer.
3. **Align daily caps with your busiest days.** Base your daily cap on your top three busiest days, plus a 10-20% buffer.
4. **Tune velocity limits to block fraud, not customers.** A typical start is no more than three attempts per card in fifteen minutes.
5. **Keep key entry tightly controlled.** Disable key entry for most front-line staff and set a low ceiling with manager override.
6. **Lock refunds to the original method with manager review.** Set a per-refund threshold for manager approval and a daily refund cap.

When to review and adjust limits

- You notice a spike in declines, chargebacks, or fraud alerts.

- You launch a new sales channel.
- Your sales patterns change due to holidays or events.
- A viral moment or media feature changes your usual traffic.

How to make changes

- **Gateway settings (you control):** Includes AVS, CVV, EMV 3-D Secure rules, and velocity limits.
- **Processor and account settings (set with ATB or Moneris):** Includes per-transaction and daily caps, refund permissions, and contactless limits.
- **To request changes or review options:** Call **1-866-433-5204** (prompt 1 for ATB, prompt 2 for Moneris).

Quarterly checklist for your team

- ☐ Export last-quarter sales, refunds, and chargeback stats.
- ☐ Compare current limits to peaks and adjust ceilings as needed.
- ☐ Test that AVS, CVV, and EMV 3-D Secure are working correctly.
- ☐ Review fraud screening and velocity rules.
- ☐ Make sure manager codes and refund permissions are current.
- ☐ Document every change and schedule your next review.

Why this discipline pays off

Strong, data-driven limits stop sudden fraud, keep disputes under control, and protect your cash flow. Regular reviews make life easier for your best customers by removing friction where you can.

Please note the following:

(a) This guide and the information it contains is provided for informational purposes only. While believed to be current and accurate, ATB makes no representations and provides no warranties regarding any of the information contained herein.

(b) ATB does not provide any form of warranty or guarantee that applying the information referenced in this guide will be wholly effective against fraud or related issues.

(c) Any complimentary resources which may be offered to impacted clients, are offered solely as a gesture of support by ATB. This offer is not an admission of fault, liability, or wrongdoing by ATB regarding any incident, and is separate from any determination under the ATB Online Banking Security Guarantee.