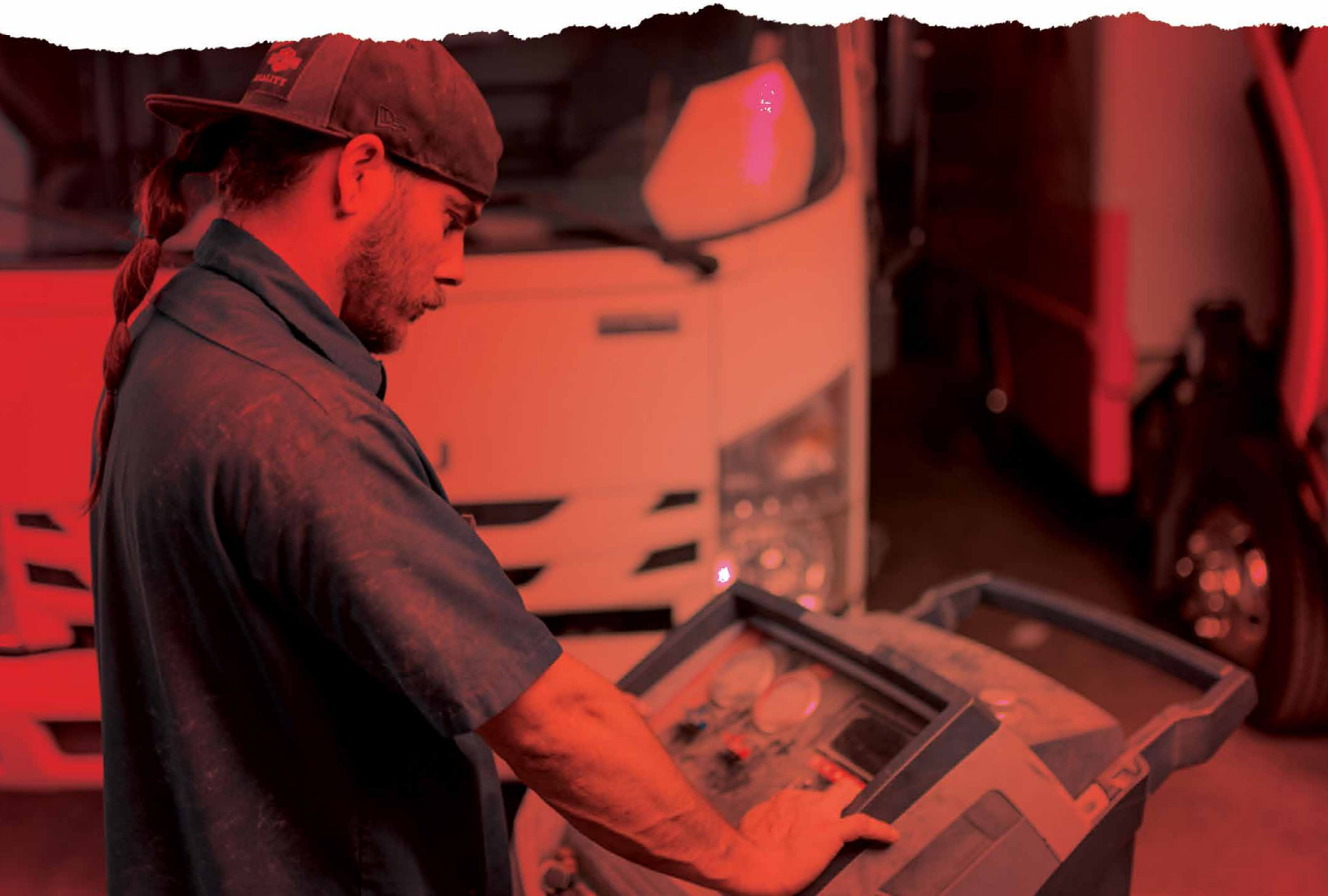
FULLBAY®

PROTECTING YOUR SHOP FROM FRAUD.



NONE OF US LIKE TO THINK WE HAVE BEEN — OR COULD BE — A VICTIM OF FRAUD.

We're smarter than that, we think. *We'll catch anyone trying to defraud us!*

Except we often don't.

Fraud happens to many businesses, including big corporations (seriously, if you walk into a restaurant and ask for the "has experienced fraud" table, you'll find heavy-duty repair right there with Amazon and Disney). Exact numbers vary; the recent *State of Heavy-Duty Repair* report revealed that **35% of shop owners have fallen victim to fraudulent activities**, but we suspect that is a low figure, as many businesses are reluctant to acknowledge they've been defrauded. But it's an unfortunate reality of running a business — *any* business — and a lot of shop owners are just not prepared for it.

The actual money lost by shops is in the millions of dollars per year, and is usually due to:

1. CREDIT CARD CHARGEBACKS
2. CREDIT CARD FRAUD
3. CHECK FRAUD
4. EMPLOYEE FRAUD AND THEFT

So, let's discuss what these fraud types entail, what they might look like in real life, and how you can protect your business. You may notice the protective measures and methods to combat fraud are similar across the four types. That's by design; some of them do share similarities, but familiarizing yourself with all of them will help you be a better shield for your business going forward.

PART I

CREDIT CARD CHARGEBACKS

A CREDIT CARD CHARGEBACK occurs when a customer disputes a charge on their credit card statement. Chargebacks in general are meant to protect cardholders from poor products and/or services, which is a great idea…until service providers have trouble fighting back against chargebacks that are the product of fraudulent activity.

Let's first make one thing clear: When you run a credit card, it's not just between you and the cardholder. You are dealing with them *and*:

- THE ISSUING BANK
- THE CARD NETWORK
- THE ACQUIRING BANK

That's five entities with their fingers in the till, and each party has its own terms and conditions.

And when a customer initiates a chargeback, their card network or bank *usually* sides with them — merchants lose 50% of all chargeback disputes.

But it's not just the money for the product or service that's lost; this study by LexisNexis states that for every $1 lost to fraud, businesses can incur as much as $4.41 in total costs, including chargeback fees, labor for managing disputes, and higher processing rates due to elevated risk profiles (yes, card companies can do that). In short, you stand to lose a lot more money than just the chargeback itself.

PETER'S TAKE

A truck was towed into my shop the day before Thanksgiving with a locked-up transmission. We diagnosed the issue, found all the needed parts, and provided a quote over the phone to the out-of-state owner.

The owner authorized the work, and we completed the repair — including a new clutch — in a single day.

The driver was thrilled, the owner was satisfied, and payment was processed via a card provided over the phone. Done and done.

But then… A chargeback notice arrived, claiming the transaction was fraudulent.

Uh-oh.

We had plenty of proof, or so we thought: emails, phone records, and a signed invoice. But we lacked concrete proof linking the owner to the truck and to the credit card used. Just like that, we lost $6,000. And even if we wanted to go after the company criminally, we had no evidence linking the guy on the other end of the phone to that truck.

IT WAS NOT ONE OF MY SHOP'S HAPPIER MOMENTS.

THE THREE PRIMARY REASONS BEHIND CHARGEBACKS

The customer claims
THEY DID NOT AUTHORIZE
the charge

The customer claims
THEY RECEIVED A PRODUCT
or service that was not as described

The customer claims
THEY WERE CHARGED MORE
than the agreed-upon price

WHERE SHOPS GO WRONG:

SATISFACTION GUARANTEES

If you have a satisfaction guarantee in your company language, drop it.

It is a tricky, dangerous phrase. You think you're doing the right thing by offering it, but in the words of Admiral Ackbar, *It's a trap*. If your customer triggers a chargeback and the term *satisfaction guarantee* appears in your paperwork, you likely will lose the chargeback. It can appear anywhere: contract, authorization forms, even your newsletters and emails — if it's there, you're setting yourself up for scammers. All a fraudster has to do is say they were not satisfied with the work and you're likely out of luck.

Your truck will be ready to pick up tomorrow at 1:00PM. See you soon!

PETER COOPER

OWNER, WIZARDLY REPAIR, LLC
SATISFACTION GUARANTEED!

WHERE SHOPS GO WRONG:

CANCELLATION/RETURN POLICIES

Your cancellation policy impacts how a credit card company rules in a dispute. This typically impacts a shop in the following way: The shop repairs the truck, the cardholder (who may be the driver or someone out of state) pays the bill, and the truck leaves the building. The cardholder then calls the credit card company — either the next day or several days later — and claims they cancelled the service and/or the parts that were used before the order was placed.

Despite having a signature on the invoice, the shop often loses the chargeback because it doesn't have a clearly stated cancellation policy. That policy is what a card company looks for when investigating chargebacks based on cancellations. If you don't have one, you're likely out of luck.

THE MORAL OF THE STORY HERE IS TO ADD STRONG LANGUAGE TO YOUR FINE PRINT THAT EXPLAINS YOUR CANCELLATION & REFUND POLICIES TO PROTECT YOU FROM CHARGEBACKS.

BOILERPLATE COPY

Use in all your invoices and estimates ***before*** you start work on a vehicle — it will help protect you against chargeback cancellations

I confirm that I have been informed and understand that all parts ordered for this specific job are non-returnable.

I further acknowledge that once the work is completed and the invoice is paid in full, no refunds or cancellations will be granted.

By signing below, I understand and accept that this is a final sale, encompassing both the non-returnability of ordered parts and the non-refundability of completed work.

Chargebacks are upsetting on many levels. They're a revenue hit, a blow to your shop's reputation, and yes, you're often left baffled, asking, "Why the heck did they do that?" Honestly, we're not going to try to dig into the psyche of the chargeback squad. We know they're out there, and we know the best way to avoid receiving a chargeback is to educate yourself and your staff on what to look for, what procedures to follow, and how to combat fraud if it ends up happening.

HOW TO PROTECT YOUR SHOP FROM CHARGEBACKS

The best way to fight a chargeback is to prevent one from happening — and that means strengthening your defenses. Set a threshold for Card-Not-Present, or CNP, transactions, if you decide to take them. Are there alternatives you could look into, like fleet checks or wire transfer? (The latter reduces chargeback risk and avoids credit card fees.) You should also familiarize yourself with other ways to protect your shop when taking CNP payments.

In addition, ***train your staff on your point-of-sale (POS) terminal***. Too many employees get brief or no training at all when new POS terminals arrive, and mix-ups like transactions and deposits being entered more than once are the stuff chargebacks are made of.

THE ABSOLUTE BEST THING YOU CAN DO, THOUGH, IS OBTAIN AND DOCUMENT PROPER AUTHORIZATION. IN THE CASE OF CNP TRANSACTIONS, YOU'LL WANT TO GO A LITTLE FURTHER.

BUILD AN AUTHORIZATION FORM

Your authorization sheet will be your secret weapon against chargebacks and credit card fraud, which we'll talk about in the next section. It should include your company name and logo, along with verbiage to the effect of "as a customer, I agree to pay X amount from this Invoice XYZ (reference the existing work order)."

Go a step further and have the cardholder put their ID and the credit card on the document and either scan it and send it to the shop, or take a picture of it and send it to the shop.

If the cardholder is not located in your area and is sending a driver to pick up their vehicle, there's an extra step you should take to protect yourself. Fullbay's Head of Payments, Mary Croy, recommends adding an "Assignment of Pickup" section or portion to the authorization form. This section should include the driver's name and a place for them to sign. You should also make a copy of their driver's license when they arrive to pick up the vehicle.

PETER'S TAKE

AS LONG AS WE USED THAT FORM, WE NEVER LOST A DISPUTE.

DOWNLOAD FREE AUTHORIZATION FORM

WHAT TO BRING TO A DISPUTE

If your shop does get hit with a chargeback and you want to fight it, you need to file a dispute. You get *one* shot to do this, so make sure you compile everything you need to prove your shop's innocence.

- THE SIGNED WORK ORDER AND SIGNED INVOICE.
- CLEAR, CONCISE RETURN/REFUND CANCELLATION POLICY SIGNED BY THE CARDHOLDER BEFORE WORK BEGAN.
- THE AUTHORIZATION FORM (DESCRIBED ABOVE) YOU HAD THE CARDHOLDER SIGN.
- PROOF OF RECEIPT — THE SIGNATURE AND DRIVER'S LICENSE OF THE PERSON WHO PICKED UP THE TRUCK, IF IT'S NOT A CARDHOLDER.
- COPIES OF THE CARDHOLDER'S ID AND THE DRIVER'S ID (IF THEY ARE DIFFERENT PEOPLE).

These are not the only strategies you can turn to for dispute prevention, but we're already running a little long. The Chargeback Gurus have an in-depth discussion of the chargeback process that you can read and are an excellent resource in general, as is Chargebacks911.

FEEL LIKE YOU'VE GOT A GRIP ON CHARGEBACKS? OKAY. GRAB A CUP OF COFFEE OR MAYBE A BEER AND KEEP SCROLLING — WE'RE MOVING ON TO CREDIT CARD FRAUD.

PART II

CREDIT CARD FRAUD

CREDIT CARD FRAUD OCCURS

when someone uses a stolen or counterfeit credit card to make a purchase. It's often tough to spot as the fraudster may actually be using a legitimate credit card…that belongs to someone else.

Here are some facts: credit card fraud was projected to reach $12.5 billion in 2024. Not great, right? In addition, 81% of all card fraud is from card-not-present (CNP) transactions — which means you should be extra alert when you deal with those types of customers.

SIGNS OF A SCAMMER

Anyone working in your shop needs to learn how to spot a potential scam-in-process. Fullbay discusses some of the signs to watch out for in this article, but make sure your staff is on the lookout for:

- **A CARDHOLDER SHOWING UP TO THE SHOP WITHOUT** their credit card on them. Do not accept the transaction.
- **A BRAND-NEW CUSTOMER MAKING A LARGE PARTS ORDER** and not indicating any sensitivity to price.
- **A CUSTOMER THAT SEEMS UNHAPPY** with the work over the phone, but still goes through with the transaction (a chargeback may be incoming)

PETER'S TAKE

A few years back, my shop received a call from an out-of-state "fleet" requesting $10,000 worth of tires. They had no brand preference and they wanted the tires ***that day.***

WE IGNORED THE FLAGS.

The next morning, a rental truck arrived. The driver remained in the cab and the "fleet owner" called and provided the card details over the phone. The transaction was approved, the tires were loaded, and the truck departed.

The store manager called me, thrilled to share that he just did a $10K counter sale. Right away, I knew something was fishy. In the words of the Fullbay marketing team, *I felt a great disturbance in the Force.*

The next day, when the U-haul showed up, I asked the driver to contact the fleet owner and have him provide a photo of his credit card and ID together.

HE SENT US A PHOTO OF A CREDIT CARD WITH HIS NAME PHOTOSHOPPED ONTO IT...

We did not sell him the tires.

Predictably, a $10,000 fraud charge followed. You would think that local law enforcement would be all over it, but unfortunately, they were not much help. So, if you think you have protection, don't count on it. Most of the time, the person committing the fraud may not even be in the country.

PROTECTING YOUR SHOP FROM CREDIT CARD FRAUD

If you don't recognize credit card fraud for what it is, you can't count on anyone else to step in for you. As always, train your staff to spot and act on red flags; much like chargebacks, credit card fraudsters will often not show any sensitivity to price or will insist on a fast transaction.

If you're not sure who you're dealing with, USDOT Safer System is a powerful way to verify the details of a company trying to pay you — use it! You should also minimize taking credit cards over the phone, especially when large sums of money are involved.

YOU SHOULD ALSO:

- **GET PROOF OF RECEIPT.** If someone besides the cardholder is picking up the vehicle, make sure you get a copy of their driver's license and have them sign something to that effect.
- **MAINTAIN A PAPER TRAIL:** Keep estimates, invoices with full names and addresses, and customer identification.
- **LOOK INTO 3DS AUTHENTICATION** It's not widely used in the U.S. yet, but it changes the liability from the merchant to the card issuer. If it's an option for you, consider using it!
- **UNDERSTAND HOW EACH CREDIT CARD COMPANY HANDLES DISPUTE MANAGEMENT.** We're providing a good primer, but each company will have its own way of conducting an investigation. For example, here are the guidelines for Visa. You'll want to familiarize yourself with the same for MasterCard, AmEx, PayPal, and any other payment processors you use.

The authorization form we talked about in the chargeback section will also serve you well for credit card disputes. *Always* have that filled out before beginning work!

YOUR SHOP'S FIRST LINE OF DEFENSE IS YOU!

Your local PD will do their best, but they are not often well-trained in dealing with fraud — especially *potential* fraud, where the crime has not yet occurred — and they may not entirely know what to do when you approach them for help. Your job is to educate yourself and know how to fight back against fraudsters.

FLEETS WILL ASK FOR VOLUME DISCOUNTS

When fleets buy a ton of product, they will normally ask for a volume discount. If someone calls you out of the blue and wants *that* much and will take whatever you have, odds are they're trying to scam you. This especially applies if you're a smaller shop — if someone wants $10K worth of CAT parts, why aren't they going straight to CAT?

PART III

CHECK FRAUD

AND SO WE COME TO CHECK FRAUD, when someone uses a stolen or counterfeit check to make a purchase, or writes a check and then issues a stop payment on it (causing the dreaded "bounced check" when you try to deposit it at your bank).

But Fullbay, you might be saying, *I don't take checks anymore…specifically so I don't have to deal with checks bouncing.*

Hey, good for you. Plenty of shops *do* still take checks, though, so this segment is for them.

So, you're depositing a check and it bounces. While it may be fraud, it may also be an honest mistake, so don't jump to the nuclear option immediately.

SIGNS OF A SCAMMER

First, reach out to the bank where the check originated from and speak to the staff. There are several reasons a check can bounce or be rejected, and a bounced check is not a crime *until* the issuer refuses to make it right.

Your next step, then, is to contact the customer and see if they are willing to write a new check. If they do not respond or refuse to pay, *then* you should file a police report. It has become fraud (and theft!).

PETER'S TAKE

BUCKLE UP, GUYS, THIS ONE'S PRETTY BONKERS.

A customer's wife stopped by the shop to pick up a truck…and as soon as she arrived, she informed us that we'd overcharged her.

We explained the service we performed and even showed her the emails authorizing the repairs. She was not happy, but she wrote the check. As soon as she left our shop, she called her bank and did a stop payment. We called her and tried to reason with her. She didn't care and would not pay the bill.

So I called the police and filed a report. To my disbelief, the local police department told me this was a civil matter. I did some research and had to send them the state statute showing that in the eyes of the law, it was shoplifting.

THAT'S HOW LITTLE CONVERSATION THERE IS AROUND FRAUD. EVEN THE COPS HAD NO IDEA IT WAS A CRIME!

The PD backed me going forward. We got on a conference call with her and the detective to inform her that anything over $1,200 in our jurisdiction was a Class D felony. She said to charge her with a crime. So he did. She was arrested, charged, and convicted, and the shop was finally paid through the state's Victims Restitution Fund.

Your state or county likely has a process to follow if a check bounces. Contact your local DA office, as most have a person who handles bounced checks. In addition, most counties have published a bad check guide that walks you through the steps you need to take to collect on a bad check — or, if necessary, how to file a criminal complaint. Here's an example from Maricopa County, AZ; they even have templated letters you can fill out and send to the check writer.

HOW TO PROTECT YOUR SHOP FROM CHECK FRAUD

There's not a lot your shop can do about customers issuing a stop pay — you can only face it after it happens — but you can be on the lookout for counterfeit checks. Train your staff to do the following, as it will help you a) spot bad checks in the making, and b) pursue fraudsters to get the money you're owed.

LOOK FOR NECESSARY INFORMATION

The check should include the payer's name, address, and bank information, along with the current date (not pre- or post-dated). Do the dollar amounts match?

VERIFY CUSTOMER IDENTITY

Record the driver's license number on the check, and photocopy the ID of the person paying by check so you can prove who issued the payment.

RECORD THE AREA

Post cameras in the area where payment is taken so you can prove the check writer was there.

KEEP SIGNED INVOICES

Always have a signed and approved invoice accompanying the check.

UTILIZE CHECK VERIFICATION TOOLS

Services like TeleCheck or Certegy can assess the risks of checks you accept.

PART IV

EMPLOYEE FRAUD & THEFT

AND SO WE COME TO the fourth type of fraud repair shops deal with: the kind perpetuated by employees. This includes stealing cash, parts, or equipment, and can result in lost revenue and damage to the shop's reputation.

How do you know if someone is stealing from you? Look at the numbers generated by your parts department — specifically the cost of the parts in your invoicing software to the cost of the parts in your accounting software. If your costs are higher in your accounting software and your inventory has not increased by that amount, ***you are buying parts that you're not selling.***

That means they are either going on trucks and not getting billed to customers…

…or they are walking out the back door.

No bueno.

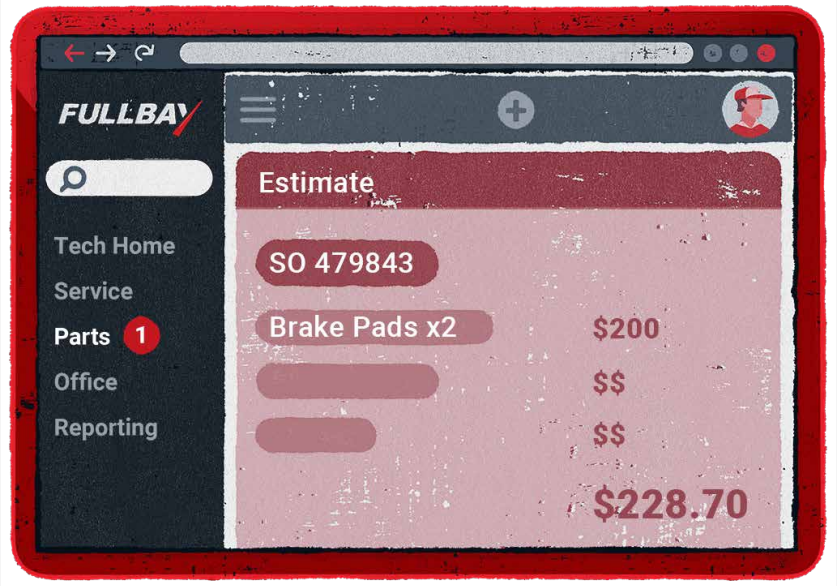
The strongest way to combat this is to lock down your shop management software, if you're using it.

Picture this: Your employee greets a customer and builds a work order in whatever shop management system they're using. They perform the work. What happens next can vary; the payer may offer them cash, or the employee may suggest a cash payment. Either way, they accept the cash, delete the work order from your software, and *poof.* All record of the transaction disappears. Your shop takes the financial hit, and the customer is none the wiser.

THE LESSON IS THIS:
IF YOU, AS THE OWNER, DON'T KNOW THE NUMBERS AND/OR WHERE YOUR MONEY IS, THEN YOU WON'T BE ABLE TO SPOT POTENTIAL LEAKS.

Lock down your software so *only* you and your managers can delete work orders.

AND ALWAYS, ALWAYS, ALWAYS USE POs.



Even if it's not all-out fraud or theft, we do find a lot of parts that employees order without a PO. They often have every intention of paying for them, but they end up lost in the shuffle and the crazy pace most small shops operate at. Your shop still takes the revenue hit, and that's not good for anyone.

Protecting your shop from the inside starts with knowing your numbers — you've got to regularly review your financial statements and inventory records. If something isn't matching up or stands out in some other way, it's time to investigate further.

We also suggest:

- **USING INVENTORY MANAGEMENT SYSTEMS** Tracking parts and preventing theft is a lot easier when you have everything digitized.
- **REQUIRING PURCHASE ORDERS.** Make sure *all* vendor purchases orders have a PO to prevent unauthorized purchases (and generally track spending).
- **CHECKS AND BALANCES:** Implement internal controls like segregation of duties and regular audits.

We'll add one more best practice, and that's to screen your employees before you hire them. There's a reason businesses conduct thorough background checks — when you hire a person, you're giving them access to your finances and, more broadly, your ability to bring in revenue. You want to make darn sure you aren't working with someone who has stolen from past employers.

CHECK YOUR ACCOUNTING SOFTWARE.

With some applications, even if you delete a work order or invoice, it still leaves a trace in QuickBooks or whatever accounting software you're using. Peter made use of this feature in his shops to catch any time an invoice was deleted, even by store managers, as they did not have access to the accounting software.

NOW DO ALL THIS WITHOUT MAKING IT DIFFICULT TO SETTLE UP

We've talked a lot about how to protect your shop from the most common types of fraud, but there's one thing we haven't discussed: how this can impact the customer experience.

To sum up, you need to keep an eye out for fraud and be prepared to combat it while making it easy for your customers to pay you. Our best advice to you is this: Be upfront. You can avoid a lot of friction by managing customer expectations. Let them know upfront that if they pay by card, you will need ID, a form, a signed estimate, and more from them. It's a single sentence that you can insert into a conversation before you start printing paperwork. And as a side note, customers that are kept in the loop tend to be happier with the completed work in general.

REMEMBER: YOU ARE YOUR SHOP'S FIRST LINE OF DEFENSE

We're not here to scare anyone — not everyone is out to get your shop. Heck, we'd even hazard to say *most* people aren't. But if it does happen to you, the financial hit may be more than your operation can bear. It makes sense to learn the signs of fraud and how to combat it.You are the first line of defense in your shop. Your awareness and the training you provide to your employees are what can protect you from bad actors.

Stay vigilant. Document everything. And in the words of Fullbay's Mary Croy, "If it sounds too good to be true, it probably is."