



An Extended Guide · No. 1913

Card Testing, Fake Refunds and Overpayment Scams Aimed at Merchants

The handful of tricks aimed at owners
— and the settings that stop them

Tech Made Simple — Service Made Personal

BillsHomeTech.com · (330) 200-8042 · Atwater, Ohio

Free & printable — share it with someone who needs it



Book a visit —
billshometech.com/book

! One rule stops most of these scams cold

If you remember nothing else: only ever refund to the ORIGINAL card and the ORIGINAL sale, and never send cash, a transfer, or a refund to a different card to settle a card payment. Nearly every scam in this guide falls apart the moment you hold that line. The rest of these pages just show you why.

Let's spot the scams aimed at merchants

Most fraud advice is written to protect the shopper. This guide flips it around and protects YOU — the owner taking the payment — from the handful of tricks that target small businesses.

I'm Bill, and I run Bill's Home Tech here in Portage County, Ohio. I've spent 30+ years helping folks with their technology, and a lot of that now is helping small shops, vendors, and home-service folks take cards without getting burned.

The good news is that these scams rely on pressure and confusion, not on clever hacking. Once you can name the trick and you've set a couple of switches in your system, you and your staff can turn almost all of them away calmly.

★ You don't need to be suspicious of everyone

The point isn't to treat every customer like a crook — most people are honest, and that's how we want to run a shop. The point is to have a few firm rules that quietly protect you from the few who aren't. Set the rules once and you can stay friendly.

The whole guide, on one page

If you remember only these things, you'll turn away most merchant scams before they cost you a dime.

- ❑ Card testing is a burst of tiny charges and declines — criminals checking stolen numbers. Turn on your processor's fraud tools, CVV and address checks, and watch for bursts.
- ❑ A fake or forced refund is someone pushing your staff to refund a card that never bought anything. Only refund to the original card and sale.
- ❑ An overpayment scam is 'I paid too much, send me the difference' — often to a different card. Never do it.
- ❑ Lock down who can issue refunds, and require a manager to approve them.
- ❑ Friendly fraud — a real customer disputing a real sale — is a chargeback; our chargebacks guide handles that one.
- ❑ Train every person who touches the register. A scam only works on staff who don't know the rule.

✓ One rule to hold onto

Money only ever goes back the way it came in — same card, same sale. If someone wants it to go anywhere else, the answer is a polite no until you understand exactly why.

Card testing — the burst of tiny charges

This one usually hits an online store or a payment link, not the counter. It's criminals using your checkout to test stolen card numbers.

Here's how it works. Someone has a long list of stolen card numbers and no idea which still work. They run them through any checkout that will take a small charge — yours, if it's handy — in a fast burst of little sales and declines. The ones that go through are the 'live' cards they'll use or sell elsewhere.

The tell is the pattern: a sudden run of small, similar charges, often a dollar or two, many of them declining, frequently in the middle of the night. Your real customers don't behave that way.

Why it costs you even though the sales are tiny

Each attempt can carry a fee, a flood of them can get your account flagged, and the successful charges often turn into chargebacks later when the real cardholder notices. A quiet burst can turn into a real mess.

! Watch for the burst

If you ever see a rush of small charges and declines you can't explain, treat it as card testing and act fast — pause online payments if you must, and call your processor. The next page covers the switches that stop it.

The settings that block card testing

You don't fight this one by hand — you let your system fight it for you. Every major platform ships tools for exactly this.

Turn on the checks that are already there

- **CVV check:** require the 3- or 4-digit code on the card. A testing bot often doesn't have it.
- **Address verification (AVS):** match the billing ZIP or address. Mismatches get declined or flagged.
- **The processor's built-in fraud tools:** Square, Clover, Toast, and Shopify all include fraud screening — make sure it's switched on, not left at the loosest setting.

Slow the bots down

- Rate limits — cap how many attempts can come from one source in a short window.
- A human check (one of those 'click the squares' puzzles) on your checkout stops automated bursts.
- Alerts on unusual activity so you hear about a burst while it's happening, not a week later.

✓ Ask your processor to tighten it

You don't have to be a tech wizard. Call your processor, say 'I want to harden my checkout against card testing,' and have them walk you through their fraud settings. Or call me and I'll sit with you while we turn the right ones on. (330) 200-8042

The fake or forced refund

This scam doesn't touch your website at all. It targets a busy, helpful person at your counter — and pressure is the whole weapon.

The play is simple: someone asks your staff to issue a refund for a purchase that never happened, or for far more than was actually bought. They may wave a receipt that isn't yours, claim a manager 'already approved it,' or create a rush so your person just wants them gone.

Sometimes it's an outsider; sometimes, sadly, it's a staff member refunding money to their own card. Either way, the money leaves your account for a sale that brought nothing in.

What makes it work

- A hurried moment — a line, a phone ringing, a new employee alone.
- Confident pressure — 'I do this all the time, just push the button.'
- No one checking the refund against a real, original sale.

! A refund needs an original sale behind it

Treat every refund request as a question: which sale is this, and can I see it in the system? If there's no matching original sale on the original card, there's no refund. Full stop.

The overpayment scam — the dangerous one

This is the trick I most want you to know, because it's aimed straight at your kindness and it can take real money.

It goes like this. A customer pays you — then says they paid too much, or a check or transfer came in for more than the bill, and asks you to 'just refund the difference.' Often they want that difference sent to a DIFFERENT card, or by cash, or by a transfer. That's the whole scam.

The original payment is on a stolen or soon-to-be-reversed card. You send the 'difference' by a route you can't claw back. Days later the original payment is disputed and vanishes — and you're out both the original amount and the difference you kindly sent.

! Never refund to a different card or method

A card overpayment gets refunded to the SAME card, for no more than the original charge, and never as cash, a transfer, or a different card. If someone pushes for any of those, you are being scammed — end the conversation and, if you've already taken the payment, call your processor.

There's no polite exception here. An honest customer who truly overpaid is fine with the money going back to the exact card they used. Only a scammer needs it to go somewhere else.

Why 'original card, original sale' beats every version

Notice that one rule defeats the fake refund AND the overpayment scam at the same time. That's not luck — it's the common thread.

Fake refunds need money to go out with no real sale behind it. Overpayment scams need money to go out by a route you can't reverse. Both die the moment you insist the refund point back to a real, original charge on the same card. One rule, two scams handled.

The ask	The safe answer
Refund to a different card	No — original card only
Send the overpayment as cash	No — back to the card only
Refund more than the sale	No — never above the original
Refund with no original sale	No — must match a real sale
Wire or transfer the difference	No — a card refunds to the card

✓ **Print the rule and post it**

Tape a small card by the register: 'Refunds: original card, original sale, never more, never cash. Ask a manager if unsure.' A sign on the wall does half your training for you.

Lock down who can issue a refund

The simplest protection is to decide, in advance, exactly who is allowed to send money back — and to make the system enforce it.

Every major system lets you set staff permissions and a refund or void approval step. Use them. When a refund needs a manager's code or login, a scammer's pressure on a junior employee stops working, because that employee literally cannot complete the refund alone.

Three switches worth setting today

- **Refund permission:** give it only to the people who truly need it, not to every login.
- **Manager approval:** require a manager code or sign-off for refunds above a small amount.
- **Separate logins:** each person signs in as themselves, so every refund has a name attached and nothing is anonymous.

! Watch refunds to the same few cards

Pull your refund report now and then and look for refunds that keep landing on the same card, or that cluster around one employee's shifts. That pattern is how most inside refund fraud finally shows up.

Friendly fraud — the real customer who disputes

One more kind deserves a mention, because people mix it up with the scams above. This is a genuine customer disputing a sale they really made.

Maybe they forgot the charge, didn't recognize your business name on the statement, or had a change of heart and found it easier to call the bank than to call you. The bank pulls the money back — that's a chargeback — and you're left proving the sale was real.

This isn't blocked by refund rules or fraud screening, because the payment itself was legitimate. It's handled with clear receipts, a recognizable name on statements, and good records. Our chargebacks guide covers how to prevent these and how to fight the ones that aren't fair.

✓ Make your name easy to recognize

A surprising number of disputes are just 'I don't know who this is.' Make sure the name that shows up on a customer's statement matches your shop's name. Our chargebacks guide shows you where to set that.

Two kinds of small business, two setups

Where you take payments changes which scam you'll meet most. A fixed counter and a seller working online or on the go face different tricks and lean on different defenses.

If you sell from a fixed counter or shop

You ring people up in one place, mostly in person, maybe with staff. Your biggest exposure is the refund counter — fake refunds and overpayment pressure aimed at a busy employee.

- Lock down refund permissions and require manager approval on refunds.
- Post the refund rule by the register and train every new hire on it.
- Use separate staff logins so every refund has a name on it.
- Review your refund report for refunds that keep hitting the same card.

If you sell on the go — markets, trucks, house calls

You sell online, by payment link, or from a booth or truck. Your biggest exposure is card testing on your checkout and overpayment scams by message or email from someone you never meet.

- Turn on CVV, address verification, and your processor's fraud screening.
- Set rate limits and alerts so a burst of tiny charges reaches you fast.
- Never refund an online overpayment to a different card or by transfer.
- If a payment-link customer overpays, refund only to the original card.

★ Not sure where you're exposed?

Most owners are a bit of both, and the mix changes which switches matter most. Tell me how and where you take payments and I'll help you set the right defenses without turning your shop into a fortress. Call (330) 200-8042.

Spotting a card-testing attack early

The faster you notice a burst, the less it costs you. Here's what a testing run looks like when it hits your account.

- A sudden cluster of very small charges, often for similar odd amounts.
- A high share of declines all at once — far more than a normal hour.
- Activity at a strange time, like the small hours of the morning.
- Lots of attempts from one place or in one short window.
- New, unfamiliar customers with no shipping and no account history.

What to do the moment you see it

- Pause online or payment-link payments if the burst is live.
- Call your processor and say you suspect card testing — they can help stop it and sort out the fees.
- Tighten your fraud settings before you turn payments back on.

✓ Set an alert so you don't have to watch

You can't stare at your dashboard all day. Ask your processor to email or text you when activity spikes, so the system taps you on the shoulder instead of you finding out from a pile of chargebacks later.

Train the people at the register

A scam only works on someone who doesn't know the rule. Ten minutes of training is the cheapest fraud protection you can buy.

Your staff are not the problem — being untrained and put on the spot is the problem. Give them clear permission to slow down, say no, and get a manager, and make sure they know they will never be in trouble for pausing a suspicious refund.

What every person who touches the register should know

- Refunds go to the original card and the original sale — nothing else.
- Never send cash, a transfer, or a different card to settle a card payment.
- 'A manager already approved it' means go find that manager, not push the button.
- Pressure and hurry are warning signs, not reasons to rush.
- When in doubt, pause and ask. No honest customer minds a two-minute check.

★ I'll help you train the crew

If you'd like, I'll come in and walk your team through these in plain English — no lecture, just the handful of rules that keep your money where it belongs. Call or text (330) 200-8042.

A note on deposits and cards on file

If you take deposits or keep a card on file — for a repair, a booking, a tab — you've got a little more to think about, and it ties into these scams.

A stored card is convenient and also a target. Keep it inside your processor's secure vault, never written on paper or typed into a notebook, and make sure a refund of a deposit follows the same rule as any other refund: back to the original card, for no more than was taken.

Overpayment scams sometimes dress up as deposit confusion — 'I put down too much, just send the extra back a different way.' Same answer as always. Our guide on deposits and cards on file covers how to store and refund these safely.

✓ Let the vault hold the card, not you

The safest card on file is the one you never see in full. Your processor's vault stores it so you don't have to, which keeps you out of trouble and makes your card-security paperwork far simpler.

What to do if one of these gets through

It happens to good, careful owners. If you've been caught, move quickly and calmly — fast action limits the damage.

The moment you realize a refund, overpayment, or testing run was a scam, call your processor. Explain what happened in plain terms. They can sometimes stop a pending transfer, flag the activity, and tell you whether a payment can still be reversed.

Then write down what happened while it's fresh — dates, amounts, what was said, any receipt or message. If money was actually taken, that record helps your processor, your bank, and if needed a police report. It also helps you fix the gap so it can't happen the same way twice.

! Don't send 'one more' payment to fix it

A common second hit is the scammer calling back to 'help resolve it' and asking for another payment or transfer. Don't. Once you know it's a scam, all further money movement goes through your processor and your bank, never the person on the phone.

The habits that keep you safe

You don't need to memorize every scam. A few steady habits catch the ones that haven't even been invented yet.

- ❑ Refunds go back the way they came — original card, original sale, never more.
- ❑ Refund permissions are limited and manager approval is required.
- ❑ Fraud screening, CVV, and address checks are switched on and tight.
- ❑ You glance at your refund and transaction reports regularly.
- ❑ Every staff member knows the refund rule and is allowed to say no.
- ❑ You keep the card on file in the vault, never on paper.

✓ Small checks, big protection

None of these takes more than a minute a day. Together they turn your shop from an easy mark into a hard one — and scammers move on to easier marks.

A settings checklist to run this week

Open your payment system and walk down this list once. Most of it takes an afternoon, and then it protects you every day after.

- ☐ Fraud screening turned on and set tighter than the default.
- ☐ CVV required and address verification on for online and keyed payments.
- ☐ Rate limits and a human check on your online checkout.
- ☐ Refund permission removed from logins that don't need it.
- ☐ Manager approval required for refunds over a small amount.
- ☐ Separate login for each staff member, no shared accounts.
- ☐ Activity alerts turned on so bursts reach you fast.

★ I'll run the checklist with you

If poking through settings isn't your idea of fun, that's exactly my kind of visit. We'll go down this list together and have your system locked down in one sitting. \$99 flat, 30-day come-back-free. Call (330) 200-8042.

Common mistakes that let scams through

Nearly every loss I hear about traces back to one of these. Knowing them in advance is most of the battle.

- **Refunding to a different card or by cash** to settle a card payment — the single costliest mistake in this guide.
- **Letting every employee issue refunds** with no approval step and no individual login.
- **Leaving fraud settings at the loosest default** because nobody ever opened them.
- **Refunding more than the original sale** or with no original sale to point back to.
- **Rushing under pressure** instead of pausing to ask a manager.
- **Never reviewing refund reports**, so inside fraud runs for months unseen.

! The one that empties the till

If you take away a single warning, make it this: never, ever send money a different way than it came in. That one habit blocks the overpayment scam, the fake refund, and most of what comes after them.

How to say no and keep the customer

You can hold every rule in this guide and still be the warm, easy-going shop people love. It's all in how you say it.

Lean on the system, not on suspicion. 'My register only lets me refund to the original card — that's just how it's set up' is friendly, true, and impossible to argue with. You're not accusing anyone; you're explaining a rule that applies to everyone.

For honest customers, that's the end of it — they're glad their money goes safely back to their own card. For a scammer, it's a dead end. Either way you stayed kind and kept your money, which is the whole goal.

✓ **Blame the policy, not the person**

'I'm not allowed to do it that way' lets everyone save face. Nobody feels accused, the honest customer is reassured, and the rule does the hard part for you.

Who to call when something looks wrong

You're not alone with this. Know your short list of who to reach before you ever need them.

Your processor is first for anything about a specific payment, refund, or burst of activity — they can see the transaction and often act on it. Your bank matters if money left your account. And for the legal fine points of a dispute, your attorney is the right call — I'm a tech helper, not a lawyer.

I fit in beside all of them: I'll help you understand what your system is telling you, set the defenses right, and sit with you while you make the call so it isn't so daunting. Plain English, same day when I can.

★ A calm second set of eyes

If something feels off and you just want someone level-headed to look at it with you before you act, that's what I'm here for. Call or text (330) 200-8042 and we'll work through it together.

Setting honest expectations

No system makes you scam-proof, and anyone who promises that is selling something. Here's what good habits really buy you.

They make you a hard target. Card testers move on to looser checkouts, refund scammers give up when there's an approval step, and overpayment tricks fail against the original-card rule. You won't stop every attempt, but you'll stop almost every loss.

Expect the occasional attempt anyway — a strange refund request, an odd message about an overpayment. That's normal. With these habits in place, it's a two-minute no, not a bad week. That's a fair trade for the small effort of setting things up right.

✓ Review it twice a year

Scams shift and so do your settings when you add staff or a website. Give this guide a quick re-read every six months and run the settings checklist again. Ten minutes keeps your defenses current.

Common Questions

The questions owners ask me most about scams aimed at merchants, answered plainly.

Q: A customer says they overpaid and wants the extra sent to a different card. Is that ever okay?

No. A card refund goes back to the same card it came from, for no more than the original charge — never to a different card, and never as cash or a transfer. An honest customer is fine with that; only a scammer needs it any other way.

Q: I think I'm being card-tested right now. What do I do?

Pause online and payment-link payments if you can, then call your processor and say you suspect card testing. Before you turn payments back on, tighten CVV, address checks, rate limits, and fraud screening.

Q: An employee swears a manager approved a big refund. Should they do it?

Not on someone's word. 'Already approved' means go confirm it with that manager in person or by their approval code. If it can't be confirmed, it doesn't happen.

Q: A real customer disputed a sale they actually made. Is that one of these scams?

That's friendly fraud, and it's a chargeback rather than a scam you block with settings. Clear receipts, a recognizable name on statements, and good records are the fix — our chargebacks guide walks through it.

★ Still unsure about something?

If you've got a refund or payment in front of you right now that doesn't feel right, don't guess — call or text me at (330) 200-8042 and we'll look at it together before any money moves.

You don't have to figure this out alone

You just have to remember that a friendly, patient person who speaks plain English is one call away.

I hope this guide made scams aimed at merchants feel a little less daunting and a lot more doable. Keep it with your other business papers, come back to a page whenever you need it, and don't feel you have to memorize a thing.

When you'd rather have a hand, that's exactly what I do. I come to your shop or your kitchen table, work at your pace, and never make you feel rushed or silly for asking. A first visit is a flat \$99, and for the parts that don't need me on-site I can often help right on your screen for \$49. Every visit comes with a 30-day, come-back-free guarantee. I don't sell payment processing and I earn no commission from any company — so the advice you get is just honest advice. For the tax and legal fine points, I'll point you to your accountant or attorney.

★ Bill's Home Tech — real help, close to home

Call or text me at (330) 200-8042, or visit BillsHomeTech.com. Serving Atwater and all of Portage County. 30+ years of patient, plain-English tech help — and if you're ever not 100% happy with a visit, I'll make it right or refund it. That's a promise. — Bill

Three Scams Aimed at Merchants

How each one works and what stops it

	How it works	What stops it
Card testing	Tiny charge burst	Fraud tools, CVV
Fake refund	No real sale	Manager approval
Overpayment	Refund elsewhere	Original card only

Pressure and confusion are the real weapon -- a firm rule disarms it.

Before You Issue Any Refund

Four checks that stop fake and overpayment scams



If any check fails, the refund waits until it clears.

The Ask Versus the Safe Answer

Money only goes back the way it came

	The ask	Safe answer
Different card	Send extra there	No
Cash or transfer	Pay it out	No
More than sale	Refund over	No
No original sale	Just refund	No

One rule defeats both the fake refund and the overpayment scam.

What Kind of Trouble Is This?

Name it, then reach for the right defense



A real customer disputing a real sale is a chargeback -- see that guide.

Illustration - a schematic, not to scale. Your setup may differ.



Need a Real Person?

You do not have to remember all of it.
You just have to remember you can call.
Friendly, in-person tech help -- I come to you.

BILL'S PROMISE

If you are not 100% happy with a visit, I will
make it right -- or refund it. No awkwardness,
no fine print. That is how I would want to be treated.

(330) 200-8042 · BillsHomeTech.com

Bill@BillsHomeTech.com · Mon–Sat 9:00 AM – 7:30 PM

— Bill

Prefer help without a visit?

Bill can screen-share and fix many things remotely — a flat \$49, free for Support Plan members.



A Note From Bill

A quick note from Bill.

I write these guides to make home tech a little less frustrating, and I do my best to keep every step accurate and up to date. Still, every home, device, and setup is a bit different, so I can't promise a guide will match yours exactly or fix your particular problem. These guides are for general information only — they're not professional, legal, or financial advice, and they don't replace your device's own manual or the manufacturer's instructions. Please go slow, use your own good judgment, and use everything here at your own risk. If a step involves electrical wiring, a gas appliance, a water heater, plumbing, or climbing a ladder — or if anything just doesn't feel safe — please stop and call a licensed professional (or give me a call at 330-200-8042). Bill's Home Tech and Bill Davis can't be responsible for any damage, data loss, or injury that comes from using these guides. Thanks for reading, and stay safe out there.

— *Bill*



Book a visit —
billshometech.com/book

Use of these guides is subject to our Terms of Use (billshometech.com/terms-of-use).

(330) 200-8042 · BillsHomeTech.com

Bill@BillsHomeTech.com · Mon–Sat 9:00 AM – 7:30 PM

For general information only — not professional advice. Use at your own risk. For electrical, gas, water, or ladder work, please call a licensed professional. — Bill's Home Tech