Welcome to the latest edition of ABTEK's monthly newsletter! Stay in the loop with our updates, insights and exciting developments in the world of payment processing. In each issue, we bring you valuable content, special offers, and a glimpse behind the scenes. Thank you for being part of our community!

Skimming, Scams & Smart Tech: How Fraud Is Changing (and How to Stay Ahead)

Fraud isn't new — but the way it shows up *is* changing. As payment technology gets smarter, so do the bad actors. Two of the biggest trends merchants are seeing right now are **card skimming** and **AI-driven fraud**.

The good news? A little awareness goes a long way.

Let's start with skimming.
Skimming happens when criminals install a hidden device on a card reader to capture card data. These devices can be surprisingly small and easy to miss — sometimes placed over a slot, inside a terminal, or even hidden in a fake keypad overlay. While skimming has been around for years, recent law-enforcement reports show it's making a comeback, especially in unattended or high-traffic environments.

Skimming red flags to watch for:

- A terminal that looks "off" or loose
- Keypads that feel thicker than usual
- Unexpected error messages or restarts
- Anything that doesn't look like it did yesterday

Encouraging **tap-to-pay or contactless transactions** can significantly reduce skimming risk — another reason those little wave symbols matter.

Now let's talk about the newer player: **AI-powered fraud.** Fraudsters are using artificial intelligence to create more convincing scams — from emails and texts that sound just like real customers, to phone calls that feel totally legitimate. AI can help criminals test stolen card numbers faster, mimic customer behavior, and exploit small gaps in payment processes.

The most common AI-assisted fraud patterns we're seeing:

- Phone orders with urgency ("I need this processed right now")
- Requests to refund to a *different* card
- Multiple attempts with slightly altered billing details

The best defense? **Pause before you process.**
Train staff to slow down, verify details, and escalate anything that feels even a little unusual. Fraud thrives on speed — caution is your secret weapon.

At ABTEK, we keep a close eye on fraud trends so you don't have to. If you ever have a transaction that doesn't feel right, give us a call. Sometimes a quick conversation is all it takes to stop a small issue from becoming a big headache.

Why Your Payment Partner Matters More Than Ever

Today's customers are choosing cards more than cash. In fact, **credit and debit cards now account for over 60% of in-store transactions in the U.S.**, with **tap-to-pay making up the majority of those payments**. Cash hasn't disappeared—but it's largely reserved for small purchases, not everyday spending. Add to that the fact that **7 in 10 consumers choose how they pay based on rewards**, and it's clear: most of your revenue is moving through card networks, not across the counter.

That's why who you trust to handle your cash flow matters. When payments are your lifeline, you need more than technology—you need a real person who answers the phone, understands your business, and cares about keeping your funds moving smoothly. At ABTEK, **local support isn't a feature—it's the foundation**.

Know a business owner who could benefit? Refer them to ABTEK and earn a $100 gift card as a Thank-You.

Over **60%** In-store transactions are paid by card

"Confidence is the most powerful form of currency."—Moira Rose

Simplifying PCI Compliance

Don't Rely on Luck—Secure Access with PCI DSS Requirement 8!

This St. Patrick's Day, while you're chasing shamrocks and sipping green drinks, make sure your system access isn't relying on the luck of the Irish! PCI DSS Requirement 8 is all about knowing *who* is accessing your systems—and making sure they're supposed to.

Just like guarding a pot of gold, you need strong authentication at every rainbow's end. That means unique user IDs, secure passwords, and multi-factor authentication (MFA) for remote access. No leprechauns sneaking in with shared logins!

So this March, make it your mission to audit user accounts, disable inactive ones, and ensure everyone accessing cardholder data is properly authenticated. Because when it comes to protecting sensitive information, luck isn't a strategy—security is.

Follow Requirement 8, and you'll be more secure than a four-leaf clover in a locked vault.

St. Patrick's Day
MARCH 17

"May good luck be your friend in whatever you do, and may trouble be always a stranger to you."
- Irish Blessing

ABTEK

ABTEK
5841 Andersonville Road
Waterford, MI 48329

ABTEK
TRIBUNE

Why Cash Back Is King — and What That Means for Merchants

In the United States, credit card rewards play a major role in how consumers choose to pay. Roughly **8 in 10 Americans carry at least one rewards credit card**, and most say rewards influence which card they pull out at checkout.

What's winning right now? **Cash back.** Consumers prefer rewards that are simple, flexible, and easy to understand — especially for everyday spending like groceries, gas, dining, and services. Unlike travel points or miles, cash back and statement credits feel immediate and tangible, which encourages customers to use their cards more often.

From the **merchant side**, this behavior can be a positive. Customers using rewards cards tend to:

- Spend more per transaction
- Choose card over cash more frequently
- Return to businesses where checkout is fast and friction-free

As rewards continue to drive card usage, merchants benefit most when payments are processed smoothly, authorization settings are optimized, and disputes are minimized. Some businesses are also exploring **card-linked offers or simple loyalty programs** to capitalize on repeat spending — without managing complex points systems.

Bottom line: understanding how customers value rewards helps merchants create better checkout experiences, reduce friction, and keep customers coming back.