

FRAUD PREVENTION FRIDAY



Friday, October 30, 2026



Debit Card Fraud Trends and Risk Mitigation for Community Banks

Source: ICBA Payments

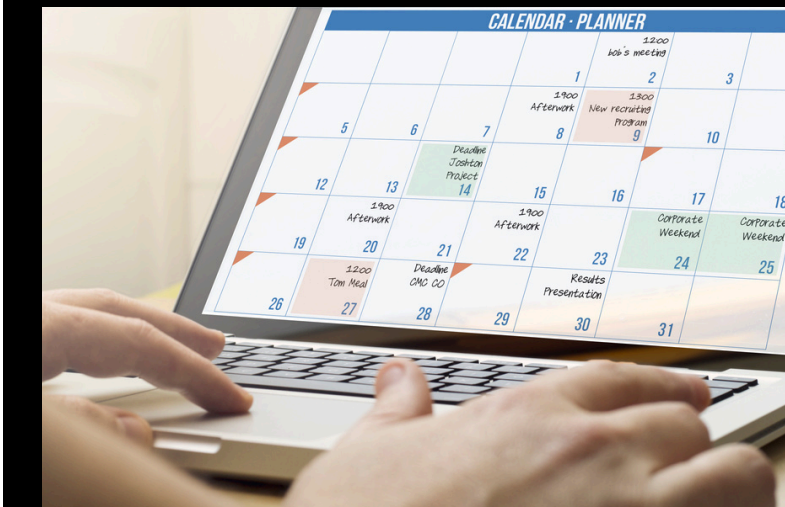
Debit card fraud remains a substantial payments risk. Federal Reserve Financial Services' 2026 [Risk Officer Report](#) found that 75% of surveyed financial institutions had encountered debit card fraud attempts during the prior year, 56% had sustained losses, and respondents attributed 40% of their payments fraud losses to debit cards. Consumer reports of bank impersonation scams, although not limited to cards, show how criminals use trusted communications to obtain credentials or induce payments.

The Federal Trade Commission received reports of about [\\$16 billion in consumer fraud losses](#) in 2025, including \$3.5 billion from impostor scams. Consumers reported nearly \$1 billion in losses to business impersonators, with bank impersonators accounting for the highest losses in that category. Some of the costliest schemes began with a false security alert and instructions to move money. Other bank impersonators [send phony fraud alerts](#) asking customers to confirm account details or share personal information. The reported losses span many payment methods, but the tactics warrant attention from card issuers because they exploit customers' trust in their banks.

(Click the heading link to read more.)

Top News

- [**Debit Card Fraud Trends and Risk Mitigation for Community Banks**](#)
- [**Warning: Attackers Are Tricking Employees Into Sharing Malicious Calendar Invites**](#)
- [**All-Green Fraud: The Invisible Threat Bypassing Your Bank's Defenses**](#)
- [**When Fraud Controls Slow the Customer Down**](#)
- [**Can CFIs Help SMBs Close the Cybersecurity Gap?**](#)



Warning: Attackers Are Tricking Employees Into Sharing Malicious Calendar Invites

Source: knowbe4

Researchers at Fortra are tracking a new variant of calendar phishing in which threat actors trick employees into sharing meeting links internally.

The attackers pose as prospective customers and contact non-sales employees, asking to be directed to a sales representative in order to discuss a business opportunity. The attacker then sends the employee a meeting link to forward to a sales contact.

- The attack takes place as follows:
- "Prospect pretext. An external sender claims they want to buy and contacts a non-sales employee for the right point of contact.
 - Helpful response. The employee engages, asks for availability, and confirms that they can route the request.
 - Internal handoff. The sender provides a meeting-booking link and asks for it to be forwarded to sales.
 - Trusted delivery. Sales representative receives the email containing a 'book a meeting' button embedded with a link, forwarded from a known colleague. The forward changes the recipient's risk calculation.
 - Calendar pivot. The booking page asks the user to choose a date and time, then introduces a Microsoft 365 work-or-school sign-in prompt, framed as necessary to complete or sync the booking."

In this last step, the sales employee is asked to enter their Microsoft 365 credentials, which is the end goal of the attack. The researchers note that this lengthy and indirect attack chain increases the effectiveness of the social...

(Click the heading link to read more.)



All-Green Fraud: The Invisible Threat Bypassing Your Bank's Defenses

Source: Independent Banker

When fraudulent transactions pass every authentication check, community banks need new strategies. Here's how behavioral biometrics, employee training, and AI fraud detection can stop what traditional security misses.

Everything about the funds transfer looked like a routine online banking session. The customer logged in using a familiar device, and the IP address matched their region. The cursor moved across the screen before hovering over the confirmation button and clicking it to initiate the transfer.

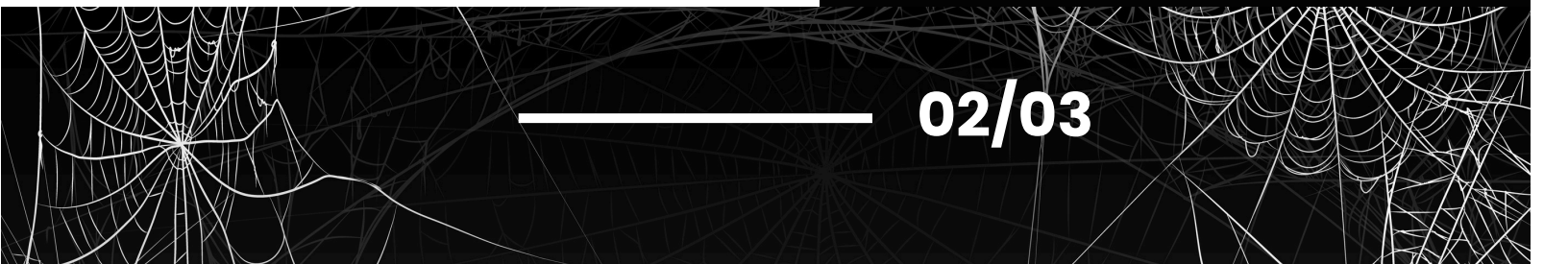
Nothing unusual here—except that the transfer was being initiated by an AI-driven bot trained to mimic the customer's online behavior. But since all the correct authentication protocols were followed, the bank's fraud monitoring dashboard gave it the green light to proceed.

What is all-green fraud in banking? It's a sophisticated scheme in which every authentication indicator—device recognition, location, credentials—shows as "green" or approved, yet the transaction is fraudulent. And it is shaping up to be one of the biggest operational challenges for community banks in 2026.

"All-green fraud is the number one fraud issue our bank is dealing with now," says Miguel Rivera, assistant vice president and fraud manager at \$3.3 billion-asset Ponce Bank N.A. in Bronx, New York.

According to the 2025 State of Fraud and Financial Crime in the United States report, conducted by PYMNTS Intelligence, account takeover fraud in which cybercriminals impersonate legitimate...

(Click the heading link to read more.)





When Fraud Controls Slow the Customer Down

Source: ProSight

Banks spent years trying to make financial transactions faster, easier, and more seamless. Fraud is complicating that push: Sometimes the safer move is to slow the customer down.

The [2026 ProSight State of Fraud Prevention Survey](#) shows that many institutions are leaning toward protection. Half of respondents said they prioritize fraud mitigation over customer experience, while 41% said they balance the two equally. Only 8% put customer experience first.

Banks are still trying to keep digital banking smooth. Fraud, though, is giving verification, scrutiny, and customer judgment a larger role in how products and payments are designed.

The survey shows the tradeoff in several places:

More verification at onboarding. One financial services leader said the institution is willing to add “appropriate friction during the onboarding process” because protecting members and their accounts is the priority. The leader acknowledged that extra verification may create “a small amount of inconvenience,” but said those steps can confirm identities, reduce fraud risk, and prevent unauthorized access.

More scrutiny before real-time payments. Real-time payments create a different kind of pressure because funds can move quickly and may be irrevocable. A BSA/AML officer at a community bank said, “With the quickness in which these payment types move, it is imperative to add additional layers of scrutiny before the funds leave the institution.” Another executive said the bank was adding controls and confirmation steps to slow users down and encourage them to validate payment details before sending money.

(Click the heading link to read more.)



Can CFIs Help SMBs Close the Cybersecurity Gap?

Source: PCBB BID Daily Newsletter

[Verizon's 2026 Data Breach Investigations Report](#) found that most confirmed breaches hit organizations with 1,000 or fewer employees, and roughly 96% of ransomware victims are SMBs. Attackers are looking for easy entry — and SMBs often provide it as they are having to manage an increasingly complex threat environment without dedicated security teams or enterprise-level resources.

The financial cost of that vulnerability can be significant. [Verizon's companion 2026 Breach Impact Study](#) found that for the hardest-hit 2.5% of SMBs, losses from a breach exceeded 7% of their annual revenue. Because SMBs operate on tighter margins than larger firms, even a modest breach can trigger a real cash flow crisis and jeopardize their ability to operate.

The gap is not just about resources; it is also about follow through. [The National Cybersecurity Alliance's 2026 Small Business Cybersecurity Awareness & Practices Survey](#) found that although most SMBs have security tools in place, they are not using them fully. For example, 86.8% use multifactor authentication (MFA), but only 51.1% require it across all key accounts. And while 88.4% have backups, just 61.4% have tested whether those backups restore.

Encouragingly, the same research also shows that there is demand for support. More than half of SMB leaders say they are likely to pursue free or low-cost training within the next six months. In addition, the most requested resources — employee training, leadership guidance on risk management, and incident response templates — suggest that businesses know they need support and guidance to strengthen their defenses.

(Click the heading link to read more.)