WSC WISCUB Service Center

BACKROOM BUZZ

March 2026 Issue 17

CRITICAL FRAUD ALERT! CHECK WASHING

We are seeing a surge in fraud across our serviced credit unions. Checks mailed to Discover card or payments going to Carol Stream, Illinois are being intercepted, washed, and fraudulently cashed or deposited.

Please alert your members immediately:

- Audit Checks: Confirm original payee remains the payee on all cleared checks.
- Go Digital: Strongly recommend online bill pay or automatic payments to avoid mail theft.
- Report Fraud: Direct victims to IC3.gov and ReportFraud.ftc.gov.

Introducing New Services!

Teller Capture

Key Benefit: Increase operational efficiency and improve the branch experience.

Thinking about moving to teller capture? Our partner's core-independent platform offers a seamless upgrade path, integrating Precision OCR (optical character recognition) and real-time fraud defense to modernize your workflow on your terms.

This flexible, browser-based option can eliminate manual bottlenecks and transform your member experience through a more efficient teller line.

Electronic Lockbox

Key Benefit: Minimize Fraud Risk by lowering exposure to lost, stolen, or altered checks.

Give your members the instant banking experience they crave. Our Electronic Lockbox turns slow bill pay into a seamless digital journey, accelerating merchant settlements to just 1-2 business days.

You can eliminate payment delays and keep your members at the center of a modern, high-speed ecosystem.

See back page for additional services and demo booking details.

Focus on Fraud

April is National Financial Literacy Month, focused on improving consumers' financial literacy and decision-making abilities, particularly in the area of fraud prevention.

(continued on back)

"Better Service Is Always A Better Value!"

Honey Stinger

What has 18 legs and catches flies?

Important Dates

WCUL Convention
Come visit us in Madison, WI
Wednesday, May 13th - Friday, May 15th

Memorial Day - CLOSED
Monday, May 25th

Juneteenth - CLOSED
Friday, June 19th

Brewers Tickets

Watch your emails for an opportunity to take in a game at American Family Field.

WCUL Leadership Institute

Congratulations to all the recent League Leadership Institute graduates!

Contact Us:

1250 W Washington Ave., PO Box 158
Cleveland, WI 53015

800 - 242 - 7660

rep@wiscubservicecenter.com

wiscubservicecenter.com Live Chat

Follow Us on LinkedIn

Introducing New Services (Continued)

These new services are designed to help modernize operations, allowing staff to spend less time on manual processing and more time focusing on members' financial well-being.

ATM Capture
ATM deposit processing and reconciliation

Traditional Lockbox
Secure next day check processing

LoanPay
Loan payment processing

To schedule a demo or learn more about these products please contact us at:

lhansen@wiscubservicecenter.com or rep@wiscubservicecenter.com
920.646.3117 or 800.242.7660
wiscubservicecenter.com - Live Chat

Honey Stinger Answer
A Baseball Team!

Focus on Fraud (Continued)

Fraud attempts targeting financial institutions have increased by more than 25%, with around 50% of these attacks now employing artificial intelligence.

Top Emerging Threats

- AI Social Engineering: Using deepfake audio/video to impersonate trusted figures.
- Synthetic Identity Fraud: The #1 threat of 2026, where "ghost" personas are built using a mix of real and fake data.
- MFA Relays: Real-time theft of security codes to bypass traditional authentication.

Advanced Security Strategies

To protect members, credit unions are shifting toward a layered defense:

- Behavioral Biometrics: Analyzing unique typing and navigation patterns to flag suspicious sessions.
- Risk-Based Monitoring: Implementing 2026 Nacha rules to audit all ACH activity.
- Zero Trust Architecture: Utilizing cryptographic identity verification for high-risk transfers.
- Targeted Playbooks: Moving from generic response plans to specific ransomware and BEC (business email compromise) protocols.

The "Human Firewall"

Technology isn't enough; members must stay vigilant by:

- Pausing & Verifying: Ignoring urgency and calling official numbers to confirm requests.
- Enabling Alerts: Monitoring real-time transaction notifications.
- Using Secure Data: Avoiding public Wi-Fi for banking.