Allied Solutions

Allied INSIGHTS

Fraud & Security RISK ALERTS

Timely insights to protect against fraud and mitigate risks

2026 TAX SEASON FRAUD

SUMMARY

Each tax season brings a measurable increase in fraud activity impacting financial institutions as members receive funds, respond to IRS communications, and engage third parties for tax preparation. Fraudsters exploit this period by impersonating government agencies, manipulating members into authorizing transactions, and using stolen identities to open accounts or redirect tax refunds. In 2026, continued reliance on digital communications and AI-enabled impersonation tactics is expected to further elevate risk across deposits, payments, and account services.

Key Tax Season Fraud Risks to Financial Institutions

- IRS impersonation scams prompting accountholders to initiate urgent payments via wires, ACH, cashier's checks, or P2P platforms.
- Phishing and smishing attacks designed to capture online banking credentials and personal identifiers.
- Refund redirection fraud including unauthorized changes to direct deposit information.
- Identity theft-driven account activity, including new account openings and fraudulent loan applications following tax filings.
- Compromised member email accounts used to submit fraudulent payment or account change requests.
- Social media-driven tax schemes leading accountholders to file fraudulent returns and attempt rapid withdrawal of proceeds.
- AI-enabled voice and message impersonation increasing the credibility of scam-related transaction requests.

Risk Indicators for Frontline and Operations Staff

- Accountholders expressing urgency or fear related to IRS demands or refund issues.
- Requests for unusual payment methods or exceptions to standard controls.
- Sudden changes to contact information or account credentials.
- New accounts or refund deposits followed by rapid withdrawals or outbound payments.
- Accountholders referencing tax advice or instructions received via text, email, or social media.

Best Practices

Strengthen transaction verification

- Apply enhanced scrutiny to tax-season wires, ACH credits, cashier's checks, and P2P transfers.
- Require call-backs to a phone number on file for at least 30 days or secondary authentication for high-risk or unusual requests.

Reinforce member authentication

- Utilize out-of-band verification for account changes and payment instructions.
- Review device, IP, and behavioral indicators for anomalies.

Enhance staff awareness

- Provide targeted tax-season fraud training for branch, call center, and back-office staff.
- Equip frontline staff with clear scripts to slow transactions and educate members.

Monitor refund-related activity

- Flag large or unexpected IRS-related deposits.
- Monitor for rapid movement of funds following refund receipt

Member education

- Proactively remind members that the IRS does not initiate contact via text, email, or social media.
- Encourage members to contact the institution directly if pressured to move funds

Incident response and reporting

- Escalate suspected tax-related fraud promptly to fraud and compliance teams.
- Report confirmed incidents to appropriate regulators and law enforcement

RISK MITIGATION RESOURCES

- Learn to recognize tax scams and fraud from the Internal Revenue Service
- View tax fraud alerts from the Internal Revenue Service
- Read the IRS impersonators consumer alert from the Federal Trade Commission
- Learn about corporate fraud and deepfake AI attacks from Cybersecurity-Insiders.com
- Visit our **NEW** Fraud Prevention Center!

Need assistance or want to request a consultation?
Contact our risk specialists at risk_specialist@alliedsolutions.net

The information presented in this email is intended for informational purposes only and should not be construed as legal advice or a legal opinion and it may not reflect the most current legal developments. You should seek the advice of legal counsel of your choice before acting on any information provided in this email.

LinkedIn