Tips and Tricks:
Fraud Prevention Checklist

How secure is your practice?

Check each statement that applies to your practice.
The more boxes you check, the more areas may require attention.

- ☐ Our email systems lack strong security controls or centralized oversight.
- ☐ Wiring or payment instructions are confirmed by email alone.
- ☐ Last-minute changes to payment details are not independently verified.
- ☐ Urgent or high-pressure payment requests are not routinely questioned.
- ☐ Email sender details and domains are not consistently reviewed for subtle variations.
- ☐ Staff are unclear on how to recognize phishing or email redirection scams.
- ☐ Links or attachments are sometimes opened without independent verification.
- ☐ Payment confirmation receipt numbers (PCRNs) are not consistently obtained or retained.
- ☐ Receipt of wired funds is not routinely confirmed with the intended recipient.
- ☐ There is no clearly documented response plan if fraud or system compromise occurs.

FCT

Tips and Tricks: Fraud Prevention Checklist

Understanding the risks and how to address them

1. Strengthen email security controls
Email accounts are a common entry point for fraud. Using systems with strong authentication, monitoring, and recovery controls can help reduce the risk of unauthorized access. Regularly reviewing account settings, including forwarding rules, can help identify unauthorized changes.

2. Verify payment instructions through a trusted channel
Confirming wiring instructions using a trusted phone number—sourced independently rather than from an email—can help prevent impersonation and redirection scams.

3. Treat last-minute changes as higher risk
Late-stage changes to payment details are a frequent fraud tactic. Pausing to independently verify these requests can help reduce exposure.

4. Slow down urgent requests
Fraud attempts often rely on creating pressure to act quickly, particularly near transaction deadlines. Building in time to verify requests can help prevent rushed decisions involving funds.

5. Review email addresses and domains carefully
Fraudulent messages often rely on small variations in email addresses or domains. Reviewing the full sender address—not just the display name—can help identify potential impersonation.

6. Support staff awareness and training
Regular training helps staff recognize phishing attempts, impersonation, verification issues, and email redirection scams, including reluctance to speak by phone or inconsistencies in documentation.

7. Verify before opening links or attachments
Links and attachments should be opened only after confirming the sender through a known and trusted contact method, especially when financial information is involved.

8. Obtain and retain PCRN documentation
A payment confirmation receipt number (PCRN) helps confirm that funds were sent and received as intended. Without it, there may be uncertainty about whether funds are final or have been redirected.

9. Confirm receipt of funds where possible
Confirming that the intended recipient has received wired funds adds an additional layer of verification and helps identify issues early.

10. Establish a clear response plan
A documented response plan—including who to contact, how to secure systems, and when to engage IT support—can help limit the impact of a suspected fraud incident.

Additional Context
Follow-up actions or coverage considerations related to wire fraud may depend on the circumstances of the transaction and whether funds were verified using best financial practices. In some situations, additional confirmation steps may be required.