



Protect Your QSR from Fraud & Cyber Disruption

FIRST first franchise capital

Cyberattacks are on the rise, with up to 88% of franchisees reporting more frequent ransomware attacks across locations in the past 12 months.¹ The best protection is to be prepared. Start with developing an Incident Response Plan (IRP) based on your franchisors' cybersecurity outline, making sure your team has defined roles and playbooks.



Step 1: Build Your Response Plan

- Align your plan with franchisor requirements.
- Assign decision makers and escalation contacts.
- Prepare for common QSR risks like POS compromise, ransomware, payment fraud, gift card fraud, and online ordering fraud.



Step 2: Isolate the Threat

- Disconnect affected POS terminals, computers, or systems.
- Disable compromised user accounts.
- Preserve logs, transaction records, and other evidence.



Step 3: Protect Payments and Operations

- Contact your bank, payment processor, POS provider, and franchisor support team.
- Consider pausing affected services, such as online ordering, delivery integrations, or gift card activity.
- Use approved backup procedures to keep stores operating when possible.



Step 4: Report the Incident

- Report fund loss or suspected payment compromise immediately.
- Notify cyber insurance, legal/compliance contacts, and law enforcement as appropriate.
- File a report at IC3.gov when applicable.



Step 5: Monitor for Related Fraud

- Review refunds, voids, discounts, chargebacks, gift cards, and loyalty activity.
- Check for unusual logins or after-hours system changes.
- Determine whether other locations may be affected.



Step 6: Keep Contacts Current

- Maintain updated contacts for your bank, POS vendor, franchisor, payment processor, IT provider, insurer, and key partners.
- Store backup contact methods outside your network.
- Confirm who can authorize emergency payments, shutdowns, or customer communications.



Step 7: Strengthen Controls

- Reset passwords and enable multifactor authentication where available.
- Remove unused or former employee access.
- Review manager permissions and update employee fraud awareness training.

¹ Yahoo Finance, "77% of Cyberattacks on Distributed Enterprises Spread to Other Locations, Systems, and Vendors," September 22, 2026.