

# ATM SAFETY BEST PRACTICES



## INTRODUCTION

Every ATM operator faces the same challenge: criminals are constantly finding new ways to target your machines. Tampering, skimming, and even jackpotting attempts are rising every year. But the good news is that many of these risks can be dramatically reduced by following a simple set of best practices.

## WHY IT MATTERS

A compromised ATM doesn't just put your revenue at risk — it erodes customer trust and can lead to expensive fines or even compliance violations. By following this checklist, you'll ensure your ATMs are harder to target, easier to monitor, and safer for your customers.

## CHECKLIST

- ☐ Change default passwords immediately
- ☐ Restrict physical access (bolts, locked enclosures, security cameras)
- ☐ Keep software/firmware patched and current
- ☐ Enable alerts and logging for suspicious activity
- ☐ Train staff to recognize skimming devices
- ☐ Rotate keys/combinations regularly
- ☐ Limit who has admin or service access

## NEXT STEPS

Following this checklist is a powerful first step toward reducing risk. But real protection comes from having a partner who monitors, services, and updates your ATMs proactively. Clear Choice Payment Solutions helps you take these best practices to the next level with advanced monitoring, stable processing, and expert support. Contact us today to learn how we can help safeguard your ATM fleet with Watchdog.

