MAVIN TECHNOLOGIES

Mavin Insights

Developed by Seibold Security and Mavin Technologies.

INTEGRATED ACCESS CONTROL FOR FINANCIAL INSTITUTION BRANCHES

Mavin Technologies is the
Cornerstone for a Comprehensive Solution

Branch Risks and Threats- Physical Security

Due to their valuable assets, bank and credit union branches face various security risks and threats. Security departments must implement comprehensive security measures to mitigate related crimes.

Some of the more prominent security threats to financial branches include:

Emerging Crime Jugging: The FBI is warning about a new crime trend called jugging, which occurs when thieves watch people take money out of an ATM or bank and then rob them, usually at gunpoint. The FBI is assisting in as many as 80 cases in 2024. It said the crime poses a significant risk to public safety and causes serious financial harm.

ATM Thefts: ATMs can be physically attacked, stolen, or compromised to skim user card data. ATM smash-and-grab crimes, although rare, are extremely violent.

Robbery and Burglary: This is perhaps the most direct threat to banks. Criminals may attempt to steal cash or valuables directly from the bank through force or stealth.

Internal Fraud: Employees may exploit their positions to commit fraud or theft. This can include skimming from customer accounts, falsifying loan applications, or manipulating bank records.

Physical Data Breaches: Sensitive documents, if not properly secured, can be physically stolen or accessed by unauthorized individuals, leading to data breaches.

Social Engineering Attacks: These involve manipulating individuals into breaking normal security procedures. This could include tailgating into restricted areas or tricking employees into providing access credentials.

Effective security measures must address these diverse threats through physical security, cyber security, employee training, and robust internal controls. Regularly updating security protocols and training employees on the latest security practices are also crucial for mitigating these risks.

Expanding on Internal Fraud

Internal bank fraud refers to illicit activities conducted by bank employees or insiders. This type of fraud can involve a range of actions aimed at stealing money or manipulating accounts for personal gain. Common forms of internal bank fraud include:

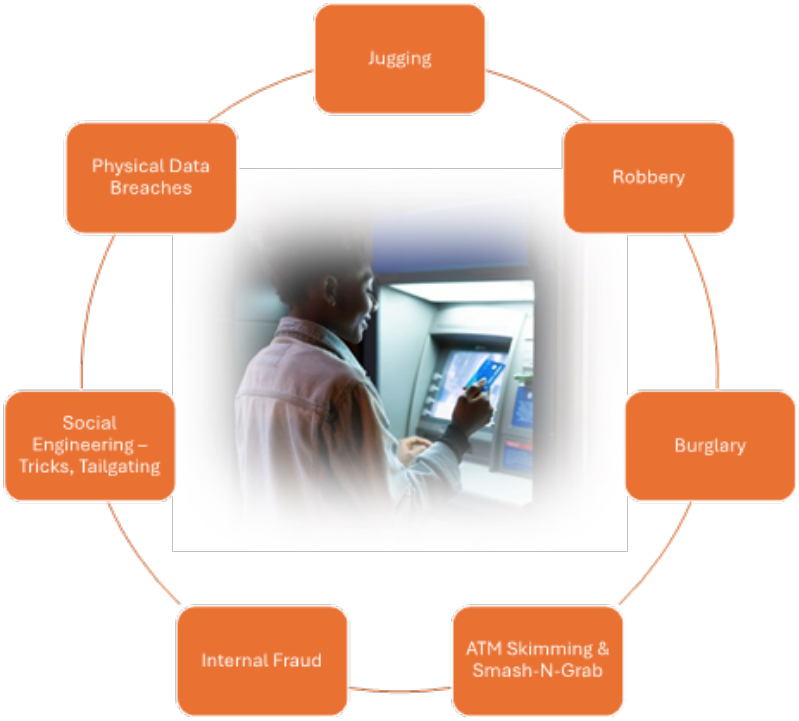
Embezzlement: Involves bank employees taking funds directly from the bank or customer accounts for personal use.

Loan fraud: Insiders may approve loans for unqualified friends or relatives or manipulate loan terms unfairly.

False accounting: Manipulating bank records to cover theft or losses or artificially inflate profits.

Theft of sensitive information: Employees may steal customer information, such as account numbers and personal data, to use or sell illegally.

Bribery and kickbacks: Employees might accept bribes to facilitate transactions that wouldn't normally be approved or to unfairly prioritize certain customers.



Internal bank fraud can be particularly damaging because it involves a breach of trust and can be harder to detect due to the insider's knowledge and access to bank systems. Banks typically employ strict internal controls, auditing procedures, and compliance measures to detect and prevent fraud.

Physical Electronic Security Branch Requirements

An integrated physical electronic security plan and deployment are crucial for ensuring the security of assets, data, and personnel. Today's access control platforms are the premiere choice for access control, integrating all other systems and sensors and achieving an automated and holistic security capability at the branch.

Branch Physical Security Solution Highlights

Access Management: Access control systems can track and control who enters the bank and specific secure areas within it. These systems often use badges or cards (physical or mobile) assigned to authorized personnel and entry points.

Security Doors and Locks: High-security doors and locks should be installed at all entry points to prevent unauthorized access. These might include biometric locks, card readers, or keypads that require a code (best served with a biometric solution).

Surveillance Systems: CCTV cameras should be installed throughout the premises to monitor and record all activities. These systems should cover interior and exterior areas, including ATMs, teller areas, vaults, and entry points.

Alarm Systems: Comprehensive alarm systems that detect unauthorized entry or suspicious activities should be installed. These systems should be connected to local law enforcement or a private security service for immediate response.

Mantraps: Double-door systems, or mantraps, control access into more secure bank areas, allowing only one person to enter or exit at a time after authentication.

Vaults and Safes: High-security vaults and safes should be used to protect cash and sensitive documents. Access to these vaults should be strictly controlled and monitored.

These controls are designed to create multiple layers of security, making unauthorized access increasingly difficult and protecting the bank's assets, information, and people.

Automation

To grasp the power of integration and automation, imagine this example...

- When a hold-up or cash drawer sensor is triggered, video cameras with analytics activate and are positioned to the proper field of view, covering the incident
- A silent alarm is sent to a central monitoring station.
- Beyond this, door locks apart from the main lobby are locked into a fail-safe mode
- ATMs are shut down in an out-of-service state.

Mavin Technologies Can Help

Mavin can help bank or credit union security leaders address overall security strategy, solutions, and risk management objectives.

Solution Highlights

- A Software Platform with many dimensions—Mavin has fully featured and integrated modules for access control, identity management, credentials issuance, alarm monitoring, action, event schedules, interactive graphical maps, real-time device status monitoring, and reports.
- Integrated with video recording, surveillance, and analytics.
- It supports integration with burglar alarms, physical branch security components and devices (Deposit boxes, teller systems, cash drawers, safes, and vaults), ATMs, fire and environmental systems, and more…

Benefit Highlights

- Realize exceptional value.
- OSDP Verified hardware – the highest security standard; know that your hardware meets the best security encryption.
- World-class support – tailored in the USA based on needs – not a script from an agent in a far-off land.
- Leverage existing investments and support industry-standard hardware from brands like Mercury and Azure - lower lifecycle costs.
- Less time to deploy – new or retrofit.
- Build business value – collaborate with HR, Risk Management, Operations, and other departments, enabling security data to enhance business processes.
- Tools like API and TAGS – Deliver greater flexibility for integrations and align with IT.
- Use IoT to raise the bar for digital transformation – wider automation, IT conformance, and interoperability.
- Easy upgrades (process, testing, training, documentation).
- Reduce risk and attain reliability - now in its fourth generation, countless satisfied customers have already standardized on Mavin.

Our customers tell us our knowledge, process, and follow-through for service are innovative and unusually comprehensive. They say we provide the highest Return on Investment and reduce the Total Cost of Ownership.

Contact a subject matter expert at financial-branch-security@go-mavin.com

MAVIN TECHNOLOGIES

12 Aqueduct Street, 3rd floor
Rochester, New York 14614
866 680.8346
info@go-mavin.com

go-mavin.com