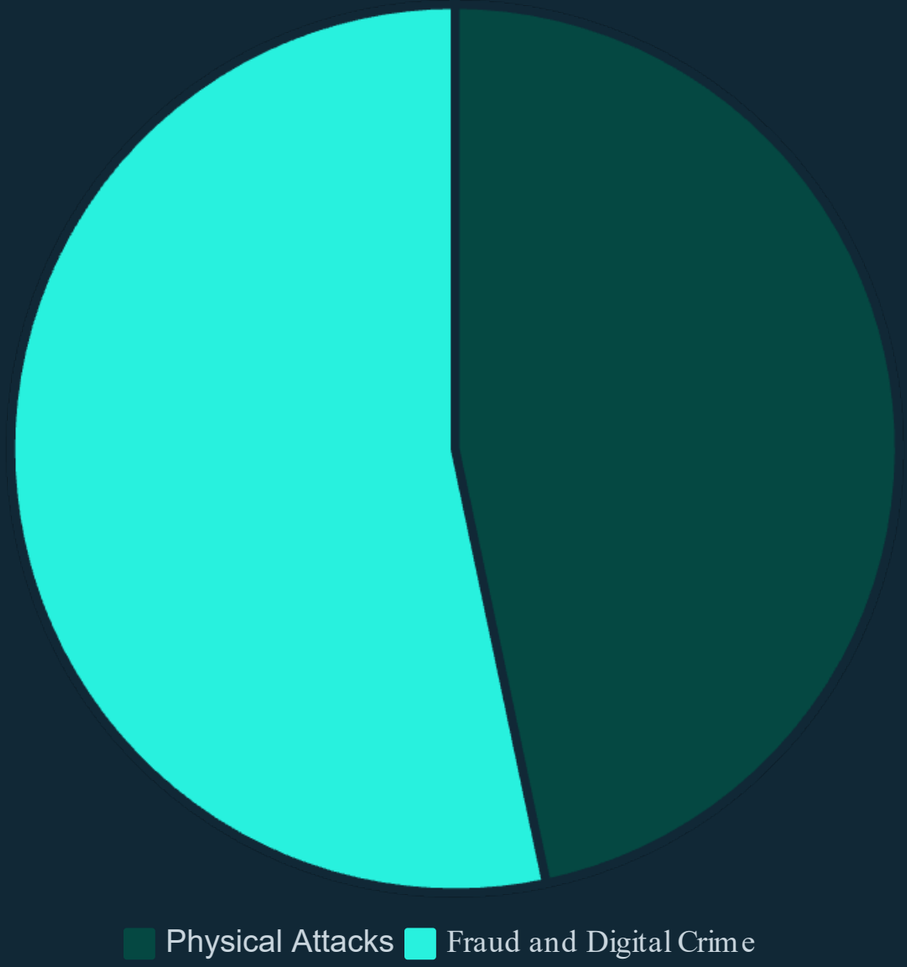
Security Best Practices: Tips to Prevent ATM Crime

ATM crime has risen over 600% since 2019. With an average of 12+ attacks per month in the U.S., it's crucial to understand and implement effective security measures.

dolphin®
DEBIT ACCESS
A Euronet Company

The Rise of ATM Crime

Physical attacks made up over 46% of reported attacks in 2024.
Fraud and "digital" crime accounted for over 53%. How can financial institutions protect their ATMs?



Curbing Physical Break-ins

1 **Reinforce Windows**

Use riot-proof glass or reinforced glazing. It's less obtrusive than steel bars and doesn't give a "bad impression".

2 **Install Bollards**

Place concrete bollards or poles in front of vulnerable areas to deter vehicular smash and grab attempts. Consider security gates for vulnerable island ATMs

3 **Secure the ATM**

Bolt the ATM to the floor. It makes removal difficult and keeps thieves onsite longer.

Curbing Physical Break-ins

4 **Security Alarms**

Install Alarms on the Top Hat and the Vault to alert authorities of a breach.

5 **ATM Processor**

Discuss alert and monitoring options with your ATM driver-processor.

Increasing Perceived Risk

Video Surveillance

Place cameras around and facing the ATM to deter criminals.

Warning Stickers

Use stickers to inform everyone they're on camera, increasing risk perception.

Signage

Let people know the ATM is monitored and suspicious activity is submitted to authorities.

Security Gates

Add security gates to your island ATMs.

Post-Attack Protection

Dye Packs

Rig dye packs to release if the ATM is jostled or exploded. Dyed money is unusable but recoverable for reimbursement.

GPS and Motion Detection

Set up GPS and motion detection to notify law enforcement during an attack. This improves response time and location tracking.

Protecting Against Sophisticated Attacks

1

Regular Inspections

Train staff to inspect machines and document their appearance to recognize new attachments or tampering.

2

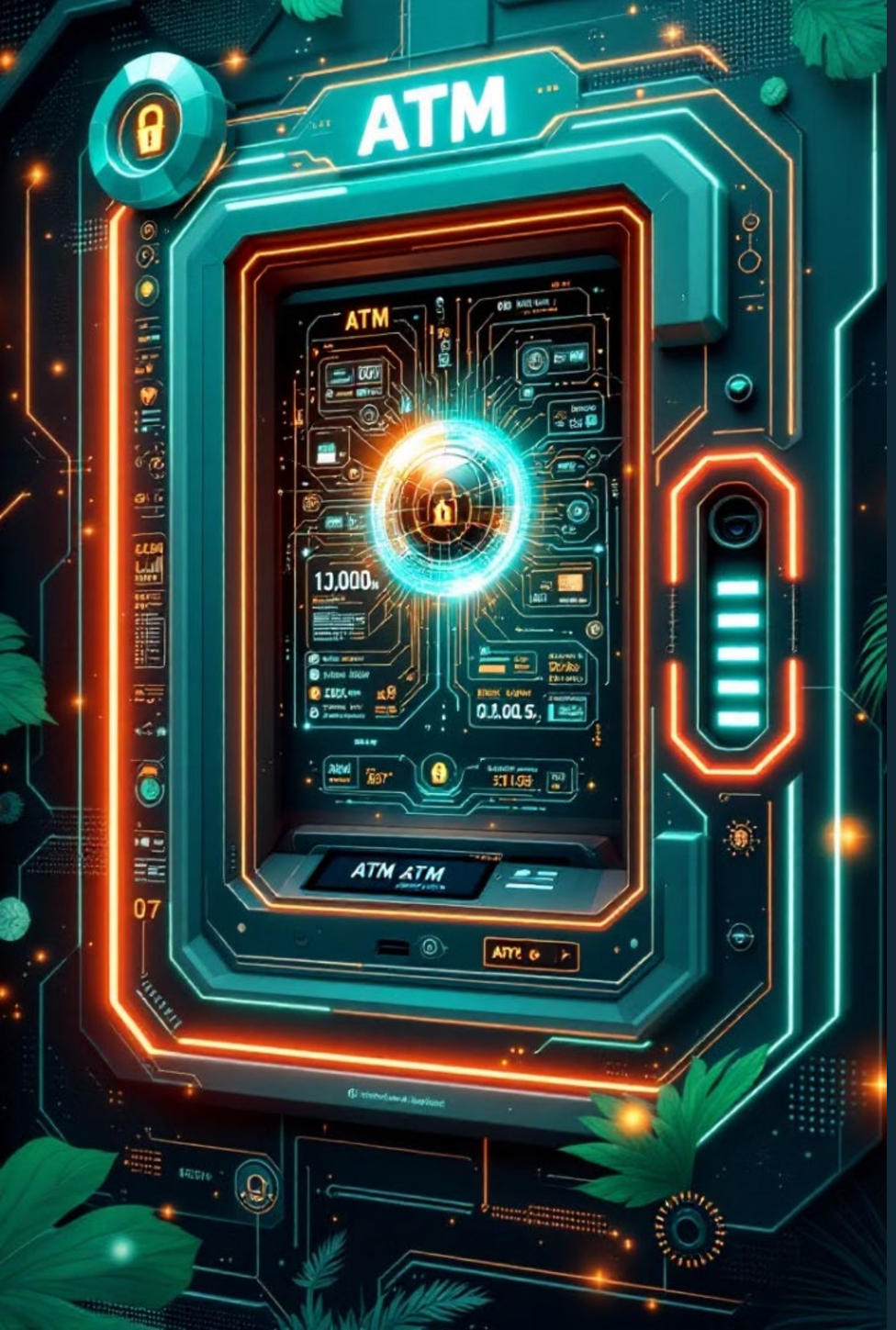
Bluetooth Scanning

Regularly scan the ATM for additional or unknown Bluetooth signals that may indicate skimming devices.

3

Secure Access Points

Ensure no exposed access points where cords or devices could be inserted to upload malicious software.



Advanced Digital Security Measures

Custom Keys

Use custom ATM keys for each machine to prevent unauthorized access with standard manufacturer keys.

White-listing

Set up the operating system to white-list only specific software and access points, preventing unauthorized uploads.

Unique Passcodes

Always update ATMs with unique passcodes before public installation to prevent easy access to operations.

Security Stack

Implement a robust software security stack to identify problems, stop malicious software, and limit access.

As a common standard Euronet introduced MSS (Multilayered Security Solution), sometimes called "Onion Model". Standard is based on the following levels of protection:

- In-house Monitoring – Euronet developed several notifications regarding unusual activity of the ATM. After receiving one of them Police or Intervention Group are notified;
  - a. Unauthorized access to ATM;
  - b. Loss of the connection;
  - c. Disconnection of dispenser module, EPP;
  - d. Sudden drop of the counters;
  - e. Usage of external device;
  - f. Access to vulnerable logical processes, and libraries on the ATM;
- BIOS protection – Administrator password plus booting only from HDD is being set
- Consider a separate VPN network for your ATM fleet. Put your firewall between the core and ATM.

MSS cont'd:

- Whitelisting:
  - a. IPS – Intrusion Prevention System which includes: USB/CD disabling, blocking unauthorized processes, traffic, access to files;
  - b. IDS – Intrusion Detection System which includes: notifications of usage of external devices; and access attempts to most important processes and dll's.
- Embedded Operational System – Image which was developed by Euronet includes the following levels of protection, e.g. no admin account, USB disabled, safe boot disabled, autorun disabled
- Constant FW upgrades – especially EPP and Dispenser;
- Windows patches – e.g. against WannaCry vulnerability;
- Communication encryption;
- HDD encryption – hard drives are being encrypted;
- PDEE (Personas Dispenser Encryption Enhancement) – introduces encryption between dispenser and PC CORE.

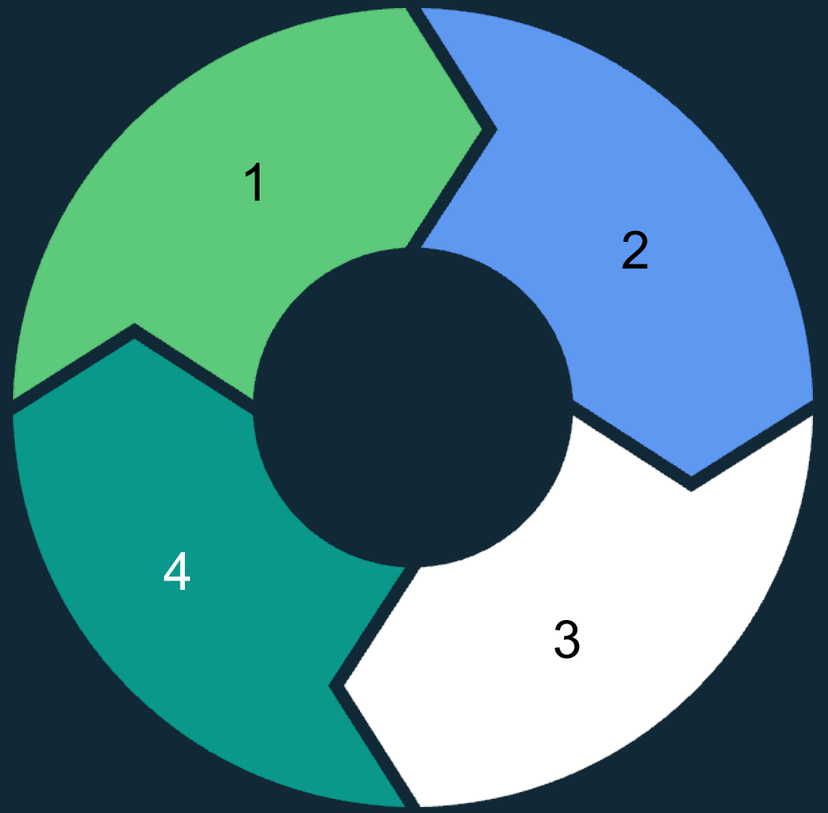
Conclusion: Deterring ATM Crime

Physical Security

Reinforce structures and implement visible deterrents.

Digital Protection

Secure software and access points against sophisticated attacks.



Continuous Improvement

Stay updated on new threats and adapt security measures accordingly.

Regular Monitoring

Conduct frequent inspections and maintain vigilance.

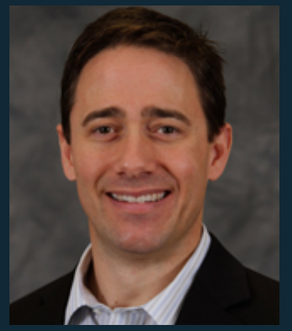
By implementing these comprehensive security measures, financial institutions can significantly reduce the risk of ATM attack and protect their assets and customers.

Thank you!

Joe Woods

SVP, Marketing & Partnerships

Dolphin Debit Access



dolphin®
DEBIT ACCESS
A Euronet Company