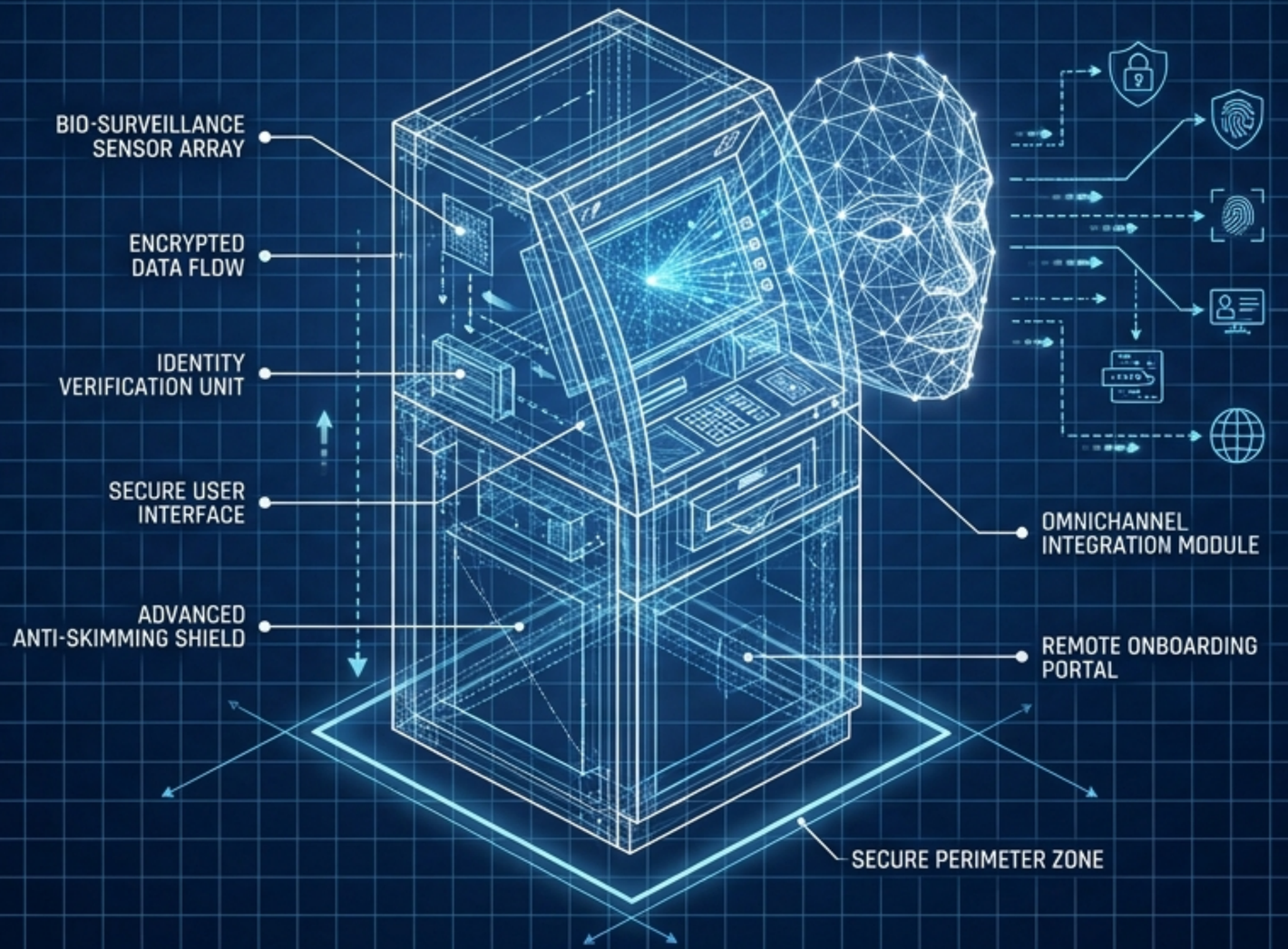
THE BIOMETRIC FIREWALL

DEFEATING ATM SKIMMING AND SCALING OMNICHANNEL IDENTITY SECURITY

AN EXECUTIVE BLUEPRINT FOR IDENTITY VERIFICATION, BIO-SURVEILLANCE, AND REMOTE ONBOARDING.



THE ANATOMY OF A COORDINATED ATTACK

1 DATA COMPROMISE

Magnetic stripes skimmed and PINs captured via concealed cameras.

2 FRAUDULENT DUPLICATION

Stolen data transferred to counterfeit cards.

3 COORDINATED EXECUTION

100 thieves deployed across Japanese ATMs simultaneously.

THE RESULT: MILLIONS OF DOLLARS EXTRACTED IN JUST THREE HOURS.

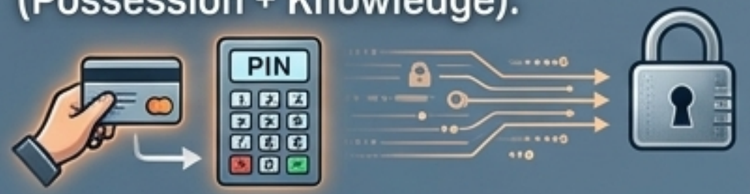
THE VULNERABILITY SCALES PERFECTLY. A CREDENTIAL COMPROMISED IN ONE LOCATION CAN BE DUPLICATED INDEFINITELY ACROSS THE NETWORK.

THE IDENTITY DISCONNECT

LEGACY PARADIGM
(Card + PIN)

AUTHENTICATION FOCUS

Focuses on valid credentials (Possession + Knowledge).



THE CORE VULNERABILITY

If a stolen card and correct PIN are presented, the system authorizes embezzlement.

THREAT RESPONSE

Reactive (discovery after funds are withdrawn).

BIOMETRIC PARADIGM
(CyberFace)

AUTHENTICATION FOCUS

Focuses on the physical user (Inherence).

THE CORE VULNERABILITY

Prevents identity duplication; system verifies actual presence.

THREAT RESPONSE

Proactive real-time identification and transaction blockage.

CYBERFACE: THE INTELLIGENT EDGE

Fast, high-quality facial recognition embedded directly into the ATM's IP camera sensor.

TRIGGER MECHANISMS

- **TRANSACTIONAL:** Triggered by card insertion or PIN entry.

- **PROACTIVE:** Triggered by environmental sensors detecting physical tampering, damage, or an active attack profile.

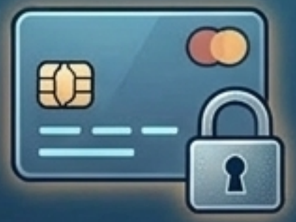
SUSPECT DETECTED

LOCKDOWN

ACTIONABLE OUTPUT: Instantly cross-references the user's face against security databases to validate identity or trigger lockdown.

THREE VECTORS OF INTEGRATION

AUGMENTED 1:1 VERIFICATION



Process: User inserts card. Camera captures face (1:1 matching).

Advantage: Adds an inherence layer to traditional card transactions.

CARDLESS BIOMETRIC

Process: Biometric identification via camera + personal code input.

Advantage: Eliminates physical skimming entirely; no card required.

MOBILE OMNICHANNEL

Process: Identification via mobile app + One-Time Password (OTP) + optional card insertion.

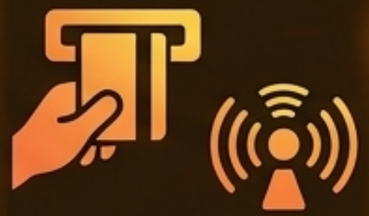
Advantage: Bridges digital and physical authentication seamlessly.

CyberFace Unified Database

THE N:1 INTERCEPT PROTOCOL

STEP 1: THE ATTEMPT

An unidentified individual inserts a stolen/forged card or triggers an ATM sensor.



STEP 2: THE CAPTURE

The IP camera automatically acquires the facial image of the user.

STEP 3: THE N:1 QUERY

The system instantly cross-references the captured image against a centralized prevention list of known suspects.

STEP 4: REAL-TIME LOCKDOWN

A match triggers an immediate alert and nullifies the transaction before funds are dispensed.

ALERT

OVERCOMING ENVIRONMENTAL FRICTION

	CHALLENGE	VS.	RESOLUTION
CHALLENGE 1: SPATIAL GEOMETRY	 Camera position and extreme face angles.		 Advanced algorithmic alignment compensates for off-axis positioning.
CHALLENGE 2: HIGH-CONTRAST ILLUMINATION	 Backlight and severe shadows.		 Dynamic range mapping extracts biometric markers despite silhouette effects.
CHALLENGE 3: DIURNAL VARIATIONS	 Fluctuating daylight vs. low-lux nightlight.		 Adaptive sensor profiling ensures consistent read accuracy 24/7.

THE TELEMETRY ARCHITECTURE

NOTIFICATION MESH (INTERNET)

Real-time alerts instantly pushed to enterprise channels (Email, SMS, Push, Slack, Web Hook, Rabbit-mq, Kafka, Amazon Lambda).

THE CORE ENGINE

Back-End Servers house the Biometric DB and Management Notifications via LAN.

DECENTRALIZED PROCESSING

Mini GPU Units process image data locally, ensuring millisecond response times without bandwidth bottlenecks.

THE EDGE

Network of ATM IP cameras capturing real-time environmental and facial data.

BEYOND THE ATM:
THE UNIFIED BIO-SURVEILLANCE PERIMETER

Building a centralized database of suspicious images does more than protect a single machine. It turns the entire branch into an intelligent, self-monitoring environment.

DATA INGESTION

The system continuously enriches its repositories via a dedicated UI, merging internal external and external camera feeds with existing databases.

EVENT HISTORY

Centralized Identification Management interface tracks all interactions.

BRANCH-LEVEL BIO-SURVEILLANCE

ENTRY CONTROL
Identify suspects from the prevention list the moment they enter the branch, long before they reach a counter.

COMPARTMENTALIZATION
Restrict sensitive building zones to authorized personnel through frictionless employee face identification.

TRAFFIC ANALYTICS
Integrate with entrance/exit sensors to calculate real-time occupancy and customer presence.

COUNTER VERIFICATION
Customer identity automatically verified upon arrival or payment at the bank counter without physical IDs.

REMOTE ONBOARDING & DIGITAL IDENTITY

Core Capability: Register entirely remotely with bank-grade biometric verification.

Document Validation: The system autonomously compares a live selfie image against a formal, uploaded certificate/ID.

FRICTIONLESS HANDOFF

THE OMNICHANNEL IDENTITY HUB

The Synthesis: A single source of truth that enables transparent hardware transitioning across the entire banking lifecycle.

THE HUB:
Certified Bank-Grade Biometrics (Proprietary Face Recognition & Fingerprint).

NODE 2: PHYSICAL FACILITIES
Securing branches via compartmentalized bio-surveillance.

NODE 1: SELF-SERVICE
Defeating skimming through 1:1 and N:1 ATM integration.

NODE 3: DIGITAL ACQUISITION
Powering remote onboarding and seamless physical-to-digital handoffs.

ENABLES TRANSPARENT HARDWARE TRANSITIONING

FROM REACTIVE FRAUD TO PROACTIVE DEFENSE

POST-TRANSACTION (REACTIVE)

PRE-TRANSACTION (PROACTIVE)

SPEED & QUALITY

Modern biometric infrastructure allows for real-time verification without adding transaction friction.

DUAL-LAYER DEFENSE

Operates proactively (triggered by sensors detecting forgery/damage) or procedurally (verifying identity alongside codes).

SCALABLE ADAPTATION

Solutions map directly to specific institutional requirements, evolving seamlessly from local ATMs to global networks.

amos@Cyberface.tech | 050-5762502