



**Mango CyberInternational, Inc.**

1234 Innovation Drive  
Tampa, FL 45678  
Phone: (555) 000-2025  
Email: mango-support@example.org

---

**Data Incident Reference: MCI-2025-10-07**

October 7, 2025

**Subject: Notice of Security Incident**

Dear Valued Customer,

We are writing to inform you of a recent privacy incident. This letter is from Mango CyberInternational, Inc., a company that provides biometric authentication solutions for organizations worldwide. Unfortunately, this event may have involved your data.

**What Happened?**

On October 7th, 2025, Mango CyberInternational identified suspicious activity within our computer systems that occurred without our authorization. We immediately took steps to stop this activity, launched an internal investigation, engaged a specialized cybersecurity team, and notified law enforcement.

Our investigation determined that a cybercriminal gained unauthorized access to a restricted area of our systems that stores encrypted biometric templates. In this type of incident—known as a biometric template attack—an adversary attempts to obtain the digital representations of users' biometric traits, such as fingerprints, facial features, or iris patterns. Once a template is compromised, it may be possible for an attacker to reconstruct or approximate the original biometric trait or to generate synthetic biometric data capable of passing authentication checks. The activity is believed to have occurred between August 10th, 2025, and September 5th, 2025.

We have no reason to believe that your data was specifically targeted. Instead, the attacker appears to have exploited system vulnerabilities in an effort to extract multiple biometric templates. Our records indicate that this process was attempted repeatedly, affecting several users enrolled across the biometric authentication systems we manage.

## **What Information Was Involved?**

We have notified our business customers of this event. The type of data that may have been viewed depends on the templates and associated records accessed by the attacker. Biometric templates stored within our systems are encrypted; however, unauthorized access to encrypted templates still presents risk if the attacker attempts to reconstruct or generate synthetic biometric data.

Based on our current findings, the information potentially accessed includes encrypted biometric templates as well as general contact information—such as name, address, date of birth, phone number, and email—and certain metadata related to recent login attempts (e.g., timestamps or device identifiers). We do not believe that financial information, passwords, or unencrypted biometric data were accessible through this attack.

## **Why Did This Happen?**

A cybercriminal targeted the storage area where biometric templates are securely maintained. This method—known as a biometric template attack—exploits vulnerabilities in template protection mechanisms to obtain stored biometric representations. Once acquired, these templates can theoretically be used to reconstruct or synthesize biometric traits that may imitate legitimate users during authentication, thereby compromising account security.

## **What Is Mango CyberInternational Doing?**

We acted swiftly to protect our systems and the individuals impacted. Our steps included:

- Disabling affected systems immediately.
- Partnering with cybersecurity experts to investigate and strengthen template protection measures.
- Enhancing encryption, integrity checks, and safeguarding mechanisms around biometric template storage.
- Increasing monitoring of all biometric authentication and template access activity.
- Notifying affected business customers and law enforcement.

## **What Can You Do?**

At this time, no additional action is required from you. However, as a precaution, we recommend:

- Remaining alert for suspicious emails, calls, or texts that may reference your personal information.
- Being cautious of unusual login requests or prompts for biometric verification.
- Contacting your institution or service provider if you suspect fraudulent use of your credentials.

## **Questions or More Information**

If you have questions or need further information about this incident, please contact Mango CyberInternational Support at (555) 000-2025 or [mango-support@example.org](mailto:mango-support@example.org) and reference Data Incident MCI-2025-10-07.

Sincerely,

Ava R. Morgan  
Chief Privacy Officer  
Mango CyberInternational, Inc.