Mango CyberInternational, Inc.
1234 Innovation Drive
Tampa, FL 45678
Phone: (555) 010-2025
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 carried out several spoofing attacks against our systems. Through these attacks, the individual successfully accessed multiple user accounts enrolled in biometric authentication systems we manage and obtained access to various accounts that our users trust us to protect through biometric verification. 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. The spoofing attacks appear to have resulted from multiple attempts to access our systems until a successful spoof was developed. Our system records indicate that this process was repeated several times, affecting multiple users enrolled across the biometric authentication systems we manage.

What Information Was Involved?

We have informed our business customers about this event. The type of data that may have

been viewed or taken depends on the specific accounts accessed by the attackers. Because we work closely with our business customers to maintain secure access across various account types, we have been assured that any systems connected to ours employ strong encryption to protect sensitive data.

Based on current findings, the information potentially accessed includes general contact information transmitted during authentication sessions—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 conducted multiple spoofing attacks designed to trick our biometric authentication systems into accepting falsified biometric inputs as legitimate. By successfully imitating genuine user verification attempts, the attacker was able to gain unauthorized access to certain accounts.

What Is Mango CyberInternational Doing?

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

- Disabling compromised systems immediately.
- Partnering with cybersecurity experts to investigate and strengthen protections.
- Enhancing monitoring of biometric authentication activities.
- 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) 010-2025 or `mango-support@example.org` and reference Data Incident MCI-2025-10-07.

Sincerely,

Ava R. Morgan

Chief Privacy Officer
Mango CyberInternational, Inc.