OLIVEPAY QUESTIONNAIRE ON " PROTECTING OLIVEPAY AGAINST FRAUD"

Section 1: AML & KYC (Financial Crime)

1. A long-time customer suddenly begins making multiple small deposits just below the regulatory reporting threshold. This is a red flag for:

A. Efficient liquidity management.
B. Structuring (a form of Money Laundering).
C. Standard retail behavior.

2. True or False: If a customer's ID looks slightly altered but they are friendly and well known to the staff, we can skip the full KYB verification process.

A. True
B. False

Section 2: Cyber Security (Phishing & Access)

3. You receive an urgent email from "Olivepay IT" asking you to click a link to "reset your password immediately" due to a breach. What is your first step?

A. Click the link to secure your account as fast as possible.
B. Forward it to your teammates to see if they got it too.
C. Hover over the sender's address to check for a spoofed domain and report it to the Security Team via the official portal.

4. When is it acceptable to share your Olivepay internal credentials or 2FA codes with a colleague?

A. only if they are a manager.
B. If you are going on vacation and they need to cover your desk.
C. Never. Credentials are individual and tied to the audit trail.

Section 3: Internal Audit & Escalation

5. If you notice a colleague bypassing a standard security protocol to "save time," what is the correct action?

A. Ignore it; it's not your department.
B. Help them find a faster way to bypass it.
C. Report the observation through the internal whistleblower/escalation channel.

6. What is the primary purpose of the Internal Audit trail?

A. To micromanage daily tasks.

B. To provide a transparent record of actions to protect Olivepay during external regulatory reviews.
C. To save storage space on the servers.