# Checklist: Senior Management

The most cost-effective way to limit the impact of payment fraud is to prevent it from occurring in the first place. This checklist is designed to help provide some key tips for keeping your business safe.

- ☐ Does your business have procedures that require validation of new or amended payment instructions? Do staff know where they can source trusted contact details?
- ☐ Do you have protocols around how, who and by what means staff can request payments to be made and how these can be verified if there are concerns?
- ☐ Are passwords of a suitable strength (e.g., minimum character lengths, use of alphanumeric characters and symbols). Have you considered using a password manager or implementing passphrases?
- ☐ Has multi-factor authentication been considered and applied where possible?
- ☐ Do your staff know what to do in the event of a fraudulent payment being sent?
- ☐ Do you have an incident response plan for cyber incidents, e.g. a compromised email address?
- ☐ Do you regularly discuss the potential risks of fraud with individuals submitting payments?
- ☐ Does your business have a policy never to share username and passwords for access to payment systems?
- ☐ Does your business have dual-transaction controls setup?
- ☐ Are junior members of the team encouraged to contact senior executives where a payment has high risk indicators?

© Hang Seng Bank



RESTRICTED