恒生銀行
HANG SENG BANK

HASE China
Payment Fraud Awareness Guide

Help protect your business against fraud & cybercrime

© Hang Seng Bank (China)

PUBLIC

Payment Fraud & Scams: protect your business

Fraud is one of the most common threats to businesses today

Payment fraud can result in significant financial losses. Businesses of every size are at risk. This guide is designed to equip you and your staff to spot and prevent payment fraud and scams, and to take the right steps if you do fall victim.

USD 1.03 TN

The Global Anti-Scam Alliance(GASA) stated that the global fraud losses in 2024 have exceeded USD 1.03 trillion.

Source: Infocast Newswire

This guide will help you learn about common fraud and scams that could impact your business and outlines some practical steps you can take to prevent your business from falling victim to fraudsters. Education on this topic across your organisation makes for a better protected business, and this guide provides a number of tips and checklists which can be shared across management and payment teams.

© Hang Seng Bank (China)

PUBLIC

Types of payment fraud & scams which could impact your business

© Hang Seng Bank (China)

PUBLIC

How a fraudster might contact you

- Authorised Push Payment (APP) scams happen when a business is tricked into sending money to a fraudster posing as a genuine payee. It's important to understand how criminals may get in touch.

- Phishing is a common theme in many frauds and scams. This describes attackers' attempts to trick users into clicking on a link that will, for example, download malware or direct them to a fake website. Phishing links may be embedded in messages received via emails, SMS or via messaging platforms.

- Vishing If you receive an unexpected phone call about money – there's a good chance it's a scam. Scammers may claim to be a business or authority you know and trust – like your bank or the police. They may know personal details about you and can even make their phone number look authentic using a technique called 'number spoofing'.

- Smishing is where scammers send fake text messages pretending to be your bank, or another legitimate organisation. Their goal is to make you reply with your personal or financial details so they can steal money from your account. Fraudsters may also utilise common messaging platforms.

© Hang Seng Bank (China)

PUBLIC

Business Email Compromise

© Hang Seng Bank (China)

PUBLIC

Business Email Compromise

Fake emails are a common tool used in scams

When payments are due, criminals send an email designed to look and read like a genuine message from a supplier. They tell you that the bank details for your payment have changed, provide new details and send a payment request.

These emails can be hard to spot:

- The attackers often use the supplier's authentic email address, or a spoofed email address which looks just like the legitimate address.
- They will make invoices look authentic.
- There may be no perceptible difference in the supplier employee's email signature.
- The message might have a sense of urgency. A common example is that the request is linked to a sensitive deal which requires a timely transfer.
- The attacker will have access to the email chain and will be able to reply using similar language and tone.
- Perhaps most importantly – often the payment they are requesting is actually due.
- Often the only difference is that the business's bank details have changed.

© Hang Seng Bank (China)

PUBLIC

How does email compromise happen?

Email account takeover

- The attacker uses hacking, or stolen account credentials, to gain access to a corporate email account.
- Account details may have been gained through a phishing attack or a data breach.
- The criminal may gather information about the user's contacts, email style and personal data to make their messages more convincing.

Email impersonation

- The criminal sets up an account with a very similar address to the real one.
- Or they may use a spoof email envelope and header, hoping the recipient will not notice and engage with it as with a legitimate message.

CEO fraud

Criminals impersonate a senior manager in the company.

- The attacker uses hacking, or stolen account credentials, to gain access to a corporate email account.
- Account details may have been gained through a phishing attack or a data breach.
- The criminal may gather information about the user's contacts, email style and personal data to make their messages more convincing.
- Ensure that, wherever possible, you only take payment instructions from approved company communication channels. Fraudsters will often contact victims via open communication channels like messaging apps.

© Hang Seng Bank (China)

PUBLIC

Account Takeover

© Hang Seng Bank (China)

PUBLIC

Account Takeover

What is Account Takeover?

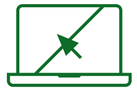
This type of fraud happens when a fraudster gains access to your bank account, typically by tricking you into divulging information, and resets your passwords and any security numbers so you cannot access your account. They may change the phone number, address and email address connected to the account; this enables them to use the account as if they were a legitimate customer.

Remote Access Takeover

This type of fraud happens when a fraudster takes control of your device and uses this control to make payments from your bank account without your knowledge or authorisation. This will usually happen after the fraudsters have sent you a link, asked you to visit a website or download a piece of software, which helps them to remotely access your device. By reading through this guide, you'll learn the tactics fraudsters use and know what you need to do to stop yourself and your business falling victim.

Number spoofing

This is where fraudsters change the caller ID (the number they're calling from), to clone or nearly clone an official number that may belong to your bank. The number may appear exactly the same or might be different by just one digit. Alternatively, they may call you from a withheld number.



Malware and Phishing

Fraudsters will use malicious software and links to steal personal information.

This information will be used to trick you into thinking a call may be genuine, or, used to hack into your bank account.

Authorization codes

No-one, including your bank, will ever instruct you how to use your physical or digital security device (also known as your secure key) or ask you for online banking authorization codes.

© Hang Seng Bank (China)

PUBLIC

Account Takeover

Recommended Tips

- Never give out your Online Banking usernames, passwords, authorisation codes, or any One Time Passcodes (OTPs).
- Remember numbers can be spoofed and never rely on the caller ID to know who's calling.
- For unexpected calls, don't be afraid to return the call using an independently verified number, such as one from the caller's official website. Use a different phone or call a known contact first to be sure the line is 'clear'.
- Be wary of suspicious emails and text messages. Especially those which contain links and ask for information. Always validate these requests with the company directly, using the contact guidance above.
- Never click on any links, visit web addresses, or download software because of a phone call you weren't expecting.
- Your security device, or secure key, is personal to you. If someone calls and asks you to use this device, end the call and contact your bank immediately.
- HSBC will never ask you to participate in an ongoing investigation, advise you how to answer questions or ask you to send your money to a safe account.
- Make sure you have a company procedure for staff to escalate concerns and ensure everyone in your business is aware of Remote Access Takeover fraud.
- Educate your staff – make sure everyone is aware of Remote Access Takeover fraud and have an escalation process in place.
- Incorporate a robust due diligence culture in your business for any payments which may include a two-tier approval process.

© Hang Seng Bank (China)

PUBLIC

How to minimise fraud risk when making payments

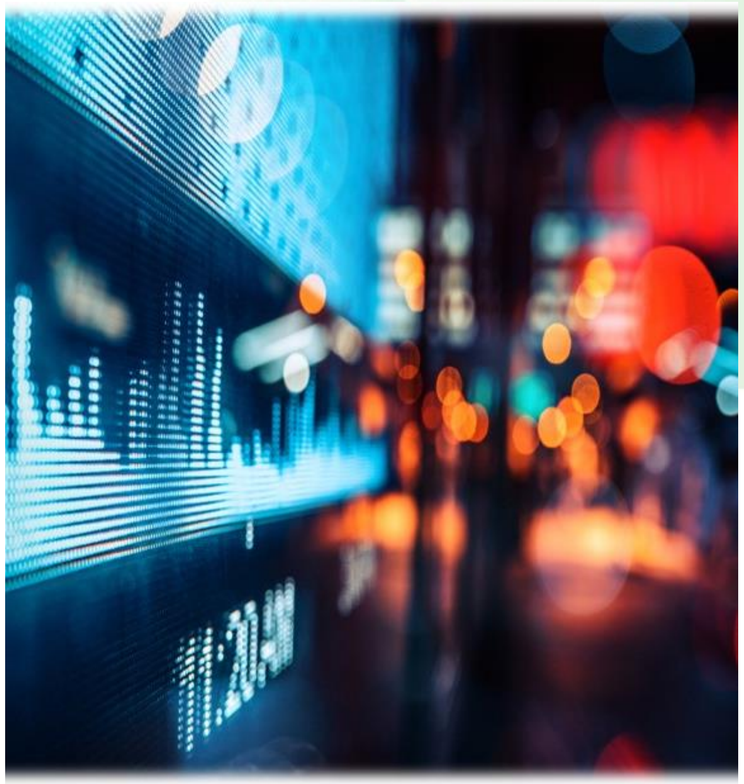
© Hang Seng Bank (China)

PUBLIC

Minimise payment fraud risk

There are steps every business can take to minimise payment fraud and scam risk that do not need to be complicated or expensive. Everyone has a role to play.

- Foster a sense of vigilance in the parts of your business that could be vulnerable.
- Educate employees about how to identify and avoid scams, and make sure they are aware of the company's security policies and procedures.
- Query any request that is unusual or out of context.
- Critically, any new payee or account details need to be verified through known sources (known contact and phone numbers) that business has established prior to the request.
- The next few slides provide more detailed guidance to support individuals responsible for payments.



© Hang Seng Bank (China)

PUBLIC

Check the email address

Fraudsters will pose as reputable individuals.

- If the name attached to the email is familiar (someone you know
  or regularly correspond with), check to be sure the email address matches.
- If it's a co-worker, the email address should be listed in the company email directory (if you have one).
- Be sure the domain name is spelt correctly. Often, fraudsters will create fake domains that closely resemble the real one, but will alter a letter or two hoping that recipients don't notice. For example, J@rnbusiness.com vs J@mbusiness.com.
- Be aware that the displayed name can be hiding the actual sender's email address.

Check the email thoroughly

Urgency is a red flag.

- Treat any email relating to payments as suspicious if it uses urgent language, or provides excuses for the lack of a call back option.
- Some phishing emails are poorly written. Even if the spelling is correct, they often contain poor grammar. Treat external emails with extreme caution, especially those containing links or attachments. Be aware that Generative AI is making it easier for attackers to create convincing malicious emails.
- If you are not expecting the communication and/or do not recognise the sender, **do not click links or open attachments**.

© Hang Seng Bank (China)

PUBLIC

Verify new payee or change of account details

Check with the instructing party using known contact details.

- Where possible, try to speak to someone you know. For example, if the change request is coming from someone within the business, try to confirm it directly with that individual via telephone. If it is from a supplier, speak to your normal contact via telephone. Remember to also check the sort code and account number.
- Don’t reply to the email or use contact details within the email or invoice.
- Often, cybercriminals are sending phishing emails to individuals in the contact lists of the account to which they’ve gained access. That means you may recognise the sender because the email address is accurate, though the message itself is suspicious. Calling your contact verifies the request in the email. It may also alert them that their email account has been compromised.

© Hang Seng Bank (China)

PUBLIC

Minimise the risk of payment fraud

Fraud can happen to any type of business and in many different ways.

Create and embed clear security procedures for payment teams

Ensuring all payments are properly validated is the most important action in fraud prevention. Create a procedure to prevent payment teams authorizing new or amended payments without proper validation. Following this procedure should mean that payment teams never move money based solely on unverified email or telephone instructions, even when they appear trustworthy. Best practice is to encourage staff to contact payees directly to confirm new or amended payment requests.

Raise employee awareness

Provide employees with adequate training. Fraud awareness is everybody's responsibility within an organization. Create a risk-based culture and have a procedure for staff to escalate concerns to management. Staff should feel able to challenge and query instructions.

Consider your digital footprint

Sharing too much information via social media platforms also allows scammers to gather information about you, your friends, family and contacts, and can be used to social engineer or impersonate you. Be less of a target by limiting the personal information you post.

Encourage all staff to think before they click

It's fine to click on links when you're on trusted websites. However, avoid clicking on links that appear in unverified emails and instant messages. If you hover over a link, you will be able to see the hidden URL and verify its legitimacy. Double check email addresses and look out for poor spelling and grammar before clicking on any links or downloading any attachments.

Strengthen your passwords

Consider password managers or using a passphrase – a string of words that is typically longer than a traditional password. Passphrases are easy to remember but very difficult to crack. Encourage employees to choose three random words and to select a mixture of alpha-numeric characters and symbols.

Know what do in an event of a fraud/cyber-attack

If you or your company fall victim, it's important to act quickly. Reporting known or suspected security incidents helps protect the workplace. Contact your financial institution.

© Hang Seng Bank (China)

PUBLIC

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 (China)

PUBLIC

Checklist: Processing Payments – 1 of 2

It is important to adopt a general mindset of awareness and action in the parts of your business that could be vulnerable. The checklist below has been created to support individuals responsible for making payments and to encourage a culture of fraud awareness.

Remember, the fraudster might have access to the inbox you are corresponding with

- ☐ **Ask yourself – is the request unusual or out of context? Does it make sense?** Any email relating to payments or accounts that uses urgent language or provides excuses for the lack of a call back option should be treated as suspicious. If you are not expecting the communication and/or do not recognise the sender, **do not click any links or open any attachments**.
- ☐ **Check that the email address is legitimate**. If the name attached to the email is familiar (someone you regularly correspond with), check to **be sure the email address matches**. Fraudsters will pretend to be reputable individuals. If it's a co-worker, the email address should be listed in the company email directory (if you have one).

  Also, be sure the domain name is spelt correctly. Often, fraudsters will create fake domains that closely resemble the real one but will alter a letter or two so that the recipients don't notice. E.g. J@rnbusiness.com vs J@mbusiness.com. Be aware that the displayed name can be hiding the actual sender's email address.
- ☐ **Question the payment if you are unsure, even if it's coming from senior management**. Fraudsters know you are more likely to act on instructions from senior individuals. As such do not trust payment instructions via email, even if they are from a senior executive or business partner. Fraudsters may also use common messaging platforms to facilitate fraud.

© Hang Seng Bank (China)

PUBLIC

Checklist: Processing Payments – 2 of 2

Verification of new and amended payment details is vital to limiting the impact of payment fraud and scams. Whilst it's important to perform callbacks, there are a number of additional considerations to ensure you minimise the risk.

Verify all new payees and all requests to change account details

Check with the instructing party using known contact details. Where possible, try to speak to the individual accountable individual for the change in details. If it is from a supplier and you speak to your normal contact, ask them to confirm with the accountable l via telephone. Remember, the fraudster might have access to the inbox of that individual, so validating the instructions via email could mean the response is coming from the fraudster!

- Don't reply to the email or invoice, use contact details within the email. If the fraudsters have gained access to soe else's account then they will likely change the contact details and you could end up speaking to thmeone fraudster.
- Call the requesting party; do not rely on them calling you. Fraudsters know that a call-back could be part of the process so might try to navigate this step by contacting you first.

Remember, the fraudster might have access to the inbox you are corresponding with

© Hang Seng Bank (China)

PUBLIC

Generative Artificial Intelligence (AI) & Fraud

© Hang Seng Bank (China)

PUBLIC

Generative AI & Fraud

Fraudsters may use generative AI to scam people and businesses

To help protect yourself, it's important that you understand the different ways that fraudsters can use the technology.

Generative AI is yet another tool that fraudsters can use to make their deception tactics more sophisticated. Given that this technology allows communication styles and likeness (video and audio) to be cloned – fraudsters can more easily impersonate people or business that you know and trust. **Some examples are below:**

- Voice spoofing – fraudster calls a member of a business pretending to be the CEO of the firm. They instruct the employee to make a 'secret' payment to a suspense account. Because the employee believes they are speaking to the CEO, they authorise the payment.
- Deepfakes – a fraudster may clone the full likeness of a member of a supplier company. Whilst pretending to be from the known supplier company, the fraudster may set up a call with the company paying for services and ask for a change in bank account details. Given that the colleague in accounts payable believes to have seen their colleague in the supplier company, they authorise the change in bank account details.

Do not assume a phone call or video call is genuine. Pay extra care if the individual is requesting sensitive information, requests you to make a payment to a new beneficiary or is making high-pressure demands.

Always have well understood procedures for paying new beneficiaries. These procedures should not be bypassed regardless of how much an employee 'trusts' the beneficiary.

What's Generative AI?

- Artificial Intelligence (AI) is technology that allows computers to perform tasks and make decisions like a human. AI tools make these decisions by learning, they do this by analysing large amounts of data and looking for patterns.
- These decisions improve as the AI tool takes in more data. With enough data, an AI tool can make decisions similar to how a human would.
- Generative AI uses similar technology to generate content. This content could be text, images, video and/or audio.

© Hang Seng Bank (China)

PUBLIC

How can you protect yourself against these threats?

Generative AI enhances a fraudsters ability deceive their victims. That said, lots of existing controls remain effective for mitigating this risk. Some key controls are noted below.

Maintain usual fraud controls

- Be mindful of emails, phone calls, and videos that want you to act quickly – this is often a sign of a scam.
- Caution against requests for personal information, account information, and financial information. HSBC will not request this information from you.
- Ensure that, wherever possible, you only take payment instructions from approved company communication channels. Fraudsters will often have to contact victims via open communication channels like messaging apps, as they are unable to access approved company channels.
- Always check and validate information you receive in emails and/or online, especially in forums or open-source websites. If you're unsure, check with a line manager or a genuine HSBC employee.

Daily Security Codes

Daily security codes are unique, time-sensitive codes generated each day and distributed to authorised personnel. These codes can be used to authenticate communications and transactions, adding a layer of security that is difficult for fraudsters to replicate. Here's how they can be implemented effectively:

- Unique Daily Codes: Generate a unique code each day to be used by employees.
- Secure Distribution: Distribute these codes via secure channels such as encrypted emails, or through internal secure platforms. Do not share codes with anyone outside of the organisation.
- Verification Processes: Require the daily code to be presented during sensitive transactions, high-value communications, or any situation where identity verification is critical.

Human Oversight & Training

- Human Oversight: Maintain a level of human oversight for approving large or unusual transactions. Conducting business in person is not always possible but, for significant transactions, can act as a key control.
- Deepfake Awareness: Educate employees about the risks of deepfakes and how they can be used in fraud schemes.
- Phishing Awareness: Provide ongoing training to help employees identify and respond appropriately to phishing attempts, which are often the precursor to more sophisticated attacks.

© Hang Seng Bank (China)

PUBLIC

Spotting A Deepfake - Additional Guidance

The rapid innovation in AI is likely to mean that deepfakes will become nearly indistinguishable from reality. Whilst these tips can help you to detect less sophisticated attacks, additional controls should be considered.

REMEMBER: Even if it looks & sounds like someone within your organisation, be sceptical if the request is unusual. It's always good to maintain a level of human oversight for approving large or unusual transactions.

1. Glasses may appear odd, reflect differently or even disappear.
2. The person's features may be positioned incorrectly or move unnaturally.
3. The person's skin or hair may appear blurry or move.
4. The audio might not sync or match the video. Listen out for changes in tone and volume.
5. The background might not fit the context of the call. It may show strange reflections or anomalies.
6. The lighting may seem off. There may be strange shadows.

© Hang Seng Bank (China)

PUBLIC

What to do if you fall victim

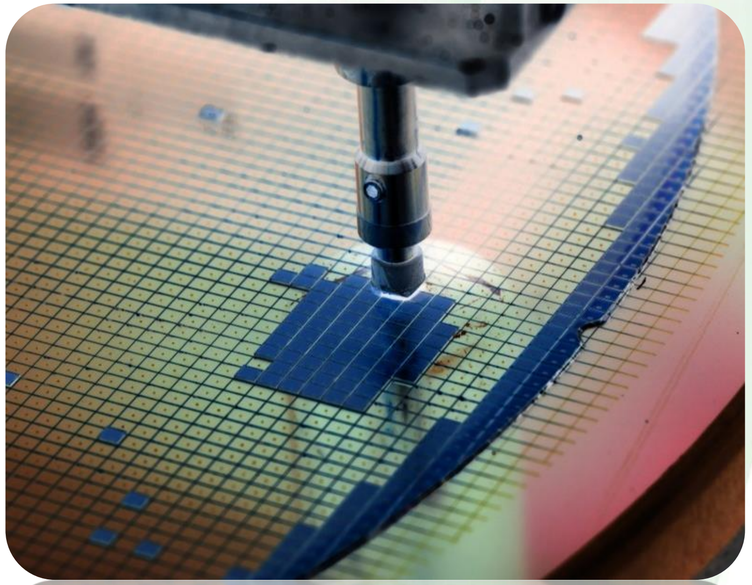
© Hang Seng Bank (China)

PUBLIC

If you fall victim to payment fraud

Act immediately to minimise the damage from fraud and to ensure the best chance of recovering funds.

- **Stop all communication** with the fraudster.
- **Alert any relevant parties** (employees, customers, and financial institutions). It is extremely important to contact the bank with a view to initiating a payment recall as soon as possible. Funds move very quickly and it can be very difficult to get funds returned once they have gone.
- **Report the fraud** to the appropriate authorities.
- **Review your financial records to identify any unauthorised transactions or suspicious activity**.
- **Keep all documentation** related to the fraud, including emails, invoices and any other correspondence.
- **Review and update your security policies and procedures.**



© Hang Seng Bank (China)

PUBLIC

Reporting fraud to HASE

If your business falls victim to fraud, it’s important to act quickly!

I received a suspicious e-mail from HASE which might not be genuine

- Stop. Don’t reply.
- Don't click on any links.
- Don't open any attachments.

You can contact our Commercial Service Hotline via:

800-830-8008 if you’re calling from Mainland China

(86)400-830-8008 if you’re calling from outside the Mainland China

I need to report fraudulent activity

If you have authorised a payment and now believe you have been the victim of a scam, or you suspect you may have divulged your security details, **call 24-hour Commercial Service Hotline immediately**.

It’s also important to inform your Relationship Manager.

Someone suspicious called me claiming to be from HASE

Someone suspicious called me claiming to be from HASE

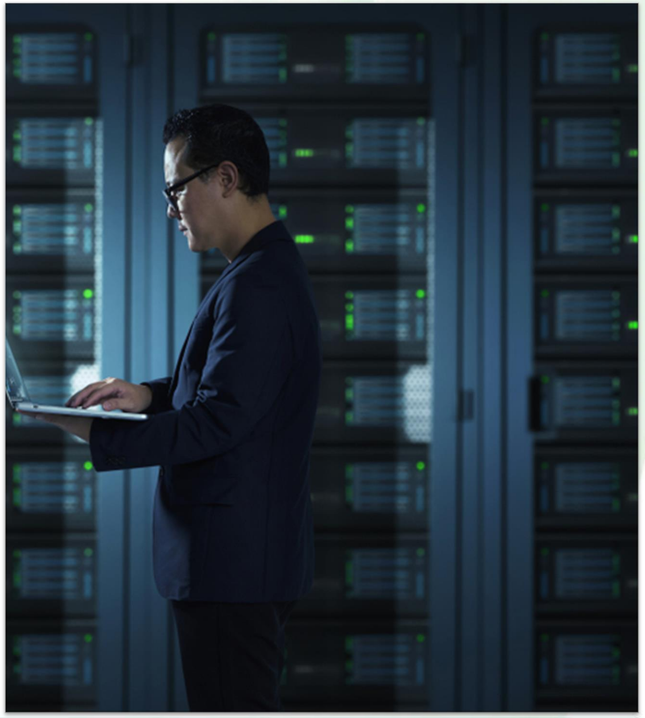
End the call and call back using a verified phone number to confirm the call is genuine. Don’t provide any information to the caller. HASE will never ask you to provide the code generated by your Security Device.

© Hang Seng Bank (China)

PUBLIC

If you suffer a cyber attack

- **Disconnect the affected devices** from the internet to prevent the spread of malware or further unauthorised access.
- **Change the passwords** for all affected accounts, including email, network, and any other accounts that may have been compromised.
- Use a reputable security firm to **conduct a full audit** of your systems to identify any other vulnerabilities or breaches.
- **Alert any relevant parties**, such as employees, customers, and regulatory authorities, and provide them with any necessary information.
- **Determine the source** of the attack and take steps to prevent similar attacks in the future.



© Hang Seng Bank (China)

PUBLIC

恒生銀行
HANG SENG BANK

Disclaimer:

This document is issued by Hang Seng Bank (China) Limited ("HACN"). The information herein is for your reference only, and which is subject to changes without notice,

No guarantee, representation, warranty or undertaking, expressed or implied is made as to the fairness, accuracy, completeness or correctness of any information or opinions contained in this document or the basis upon which any such opinions have been based and no responsibility or liability is accepted in relation to the use of or reliance on any information or opinions whatsoever contained in this document. You must make your own assessment of the relevance, accuracy and adequacy of the information and opinions contained in this document and make such independent investigations as you may consider necessary or appropriate for the purpose of such assessment. If any content in the document is marked as being quoted, summarized or translated from any third-party report, such content is for your reference only and shall not be relied upon or regarded as accurate and comprehensive restatement of such report. You can seek direct access to such research report via web-link attached in the document or other source/channel indicated in the document for more details.

HACN does not provide legal, tax, accounting, regulatory or other specialist advice and you should make your own arrangements in respect of such matters accordingly. In particular, this document may contain certain references to regulation. HACN makes no representation that the references to regulation, if contained herein, are exhaustive. There could be other references to regulation that may also be relevant to the proposals. HACN does not give advice on regulation. You should consult your own advisers on regulation.

© Copyright Hang Seng Bank (China) Limited [2026] ALL RIGHTS RESERVED. No part of this document may be reproduced, stored in a retrieval system, or transmitted, on any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without the prior written permission of Hang Seng Bank (China) Limited.