NOTICE TO MEMBERS

Notification of Cyber Intrusion to Club Servers

Dear Member,

I am writing today to inform you of a cyber intrusion discovered on 3rd August 2020 that affected the Club, explain what this means for you and certain precautionary measures you can take, and detail what steps we are taking to address the issue and safeguard those whose data may potentially have been at risk.

A full investigation led by third party cybersecurity experts, including forensic IT investigators, is ongoing. Significant findings relevant to the intrusion have been uncovered, which we outline below.

We wanted to notify all members as early as possible, even though the investigation has not yet concluded, so that appropriate precautionary actions can be taken. We will be sharing further details as the forensic investigation progresses.

What Happened?

The IT systems of the Club were subject to a ransomware attack on Monday 3rd August. The attacker encrypted files on our servers and shared an extortion message, threatening only to decrypt them in return for a ransom payment. The attacker has also indicated that it has exported certain data.

The Club was able to quickly recover the vast majority of data from backup servers, with limited impact to the Club's operations. You may have noticed that there has been some impact to the car parking system. We apologise for any inconvenience caused to you by the impact on this, or any other of our systems.

The Club, along with our third-party experts, has located, isolated and taken steps to block the ransomware from continuing to operate.

What Information Was Affected?

While it appears that the vast majority of affected data involved day-to-day administrative and operational files, member data was also among the information encrypted by the attacker.

We have no indication that any member data was exported from our systems, but it appears that basic member data was among the data that may have been at risk. This information consists of names, contact details (email addresses and phone numbers), dates of birth, and Hong Kong ID numbers of Club members and family members. According to our findings so far, financial data (i.e. bank or credit card details) and addresses of members

Notification of Cyber Intrusion to Club Servers

and family members **was not** among the data we currently understand may have been at risk of extraction by the attacker.

While it is not yet clear if any member data was in fact exported from the Club's servers, we are encouraging all members to take a number of steps to safeguard themselves. We are also in the process of identifying a trusted identity monitoring firm to provide you with identity protection services at no cost to you.

What Actions Have We Taken?

Upon detecting the intrusion, we immediately secured our servers, engaged with leading cybersecurity experts, and initiated an extensive and thorough investigation of the event. We also notified relevant law enforcement agencies by filing a complaint with the HK Police and, through our cybersecurity experts, contacting the FBI.

We have immediately taken a number of measures recommended by the forensic IT experts to protect the Club against any similar incident occurring in future. These measures include:

- Locating and taking steps to block the malware from continuing to operate;
- Activating a cloud based anti-virus and phishing detection service;
- Resetting passwords and user accounts;
- Performing a review of all user accounts to ensure all accounts are related to an active user; and
- Deploying predictive security platforms to all systems in the Club's IT network to make predictions about and provide protection from current, future, and unknown attacks.

After gathering key details of the incident, we have taken steps to notify potentially affected parties, including you, at an early stage while the forensic investigation continues. We will continue to actively communicate with all members and potentially affected individuals.

The Club takes cybersecurity seriously and has continuously invested in infrastructure to protect our systems from cyber-attacks. Unfortunately, there is no way to entirely guard against threats of this nature.

Going forward, we will continue to adhere to the strictest industry standards of data protection and will seek expert advice on ways we can further enhance the Club's cybersecurity resilience.

Notification of Cyber Intrusion to Club Servers

What Can You Do?

While it is not yet clear whether member data was exported from the Club's servers, and while we have not found that financial data or addresses of members or their family members were among the data that may have been at risk of being exported by the attacker, we would recommend that members consider taking the following precautionary actions for themselves and their family members:

- Monitor accounts that use personal data;
- Change the login credentials for online accounts, including but not limited to those used to access Club facilities and online members' area;
- Use strong passwords and change them regularly. Try to keep password at least eight characters long and use numbers, upper case, lower case and symbols;
- Enable two-factor authentication on all your online services where possible;
- Be suspicious if anyone contacts you by email, phone call or text message asking you to confirm your personal details. Never give out personal details unless you're sure who you're speaking or writing to; and
- Check your bank and credit card statements regularly for any unusual payments that you don't recognise.

I fully understand and appreciate your concern regarding this matter, and we apologise for any inconvenience this causes you. Should you have any questions about this matter, we ask that you contact the Club on **cyberenquiries@hkfc.com**.

We will endeavour to keep all members up to date as further information comes to hand.

Yours Sincerely,

Chairman
Hong Kong Football Club

20Aug2020