

Phishing emails and fraudulent websites related to Alipay Financial Services (HK) Limited

The following is issued on behalf of the Hong Kong Monetary Authority:

The Hong Kong Monetary Authority (HKMA) wishes to alert members of the public to a [press release](#) issued by Alipay Financial Services (HK) Limited relating to phishing emails and fraudulent websites. The relevant stored value facility (SVF) licensee has reported the case to the HKMA.

The phishing emails and the fraudulent websites reported by the SVF licensee known at the time are as follows:

AliPayID@contact[.]com
noreply@campaign[.]evenbrite[.]com
alipayhk@contact[.]hk
aliaycHK@contact[.]com
alipayhkDispatch@contact[.]com
[https://alopayhkgateway\[.\]com/](https://alopayhkgateway[.]com/)
[https://sonhkali\[.\]com/](https://sonhkali[.]com/)
[https://alosown\[.\]com/](https://alosown[.]com/)
[https://alipoyboost\[.\]com/](https://alipoyboost[.]com/)
[https://alipoyforge\[.\]com/](https://alipoyforge[.]com/)
[https://alipoysync\[.\]com/](https://alipoysync[.]com/)
[https://alopoyexper\[.\]com/](https://alopoyexper[.]com/)
[https://alopayhkventure\[.\]com](https://alopayhkventure[.]com/)
[https://alopayhkconnect\[.\]com](https://alopayhkconnect[.]com/)
[https://swuinsori\[.\]com/](https://swuinsori[.]com/)
[https://alopayhktech\[.\]com/](https://alopayhktech[.]com/)
[https://alipoylink\[.\]com/](https://alipoylink[.]com/)
[https://hkainlo\[.\]com/](https://hkainlo[.]com/)
[https://nohkalis\[.\]com/](https://nohkalis[.]com/)
[https://alistoeshk\[.\]com/](https://alistoeshk[.]com/)
[https://unkhkso\[.\]com/](https://unkhkso[.]com/)
[https://alipoyscape\[.\]com/](https://alipoyscape[.]com/)
[https://cnpayalo\[.\]com/](https://cnpayalo[.]com/)
[https://hkpayalise\[.\]com/](https://hkpayalise[.]com/)
[https://sarnopay\[.\]com/](https://sarnopay[.]com/)
[https://alistoeshk\[.\]com/1/](https://alistoeshk[.]com/1/)
[https://alipoystream\[.\]com/](https://alipoystream[.]com/)

The HKMA wishes to remind the public that anyone who has provided his or her personal information or account credentials, or who has conducted any financial transactions, through or in response to the emails and the websites concerned, should contact the relevant SVF licensee, and report to the Police or contact the Anti-Deception Coordination Centre of the Police at 18222.