

## School & Parent Notice

Dear Parent/Carer,

Wisepay informed us yesterday evening (7<sup>th</sup> October) at 11.05pm that at some point around 2 October 2020, a cyberattack occurred in the form of a URL manipulation, meaning that the Wisepay's payment gateway page was redirected or controlled by a bad actor, and your payment card data may have been unlawfully disclosed.

**Wisepay have informed us that some of our parents attempted to make a card payment during this period and therefore may have been affected. We are contacting Wisepay as a matter of urgency to support them in directly alerting those parents who are affected. We will contact you directly if Wisepay tell us that they believe you have been affected, and share any additional information that Wisepay provide us with in this case.**

Wisepay have asked us to share the following information with you.

WisePay has engaged a computer forensics expert and the forensic investigation is ongoing. We recommend that you are especially cautious regarding your personal financial arrangements and take prompt steps to pause or cancel the payment card you used on our site. We also recommend you take additional precautionary steps to change passwords or login details for your bank accounts and credit cards.

Some indicators that suggest your personal data may have been compromised are as follows:

1. You have suspicious transactions on your payment card statement.
2. You get a ransomware message.
3. You get a fake antivirus message.
4. You have unwanted browser toolbars.
5. Your search history is unfamiliar.
6. Your internet searches are redirected.
7. You see frequent, random popups onscreen.
8. Your friends receive social media invitations from you that you did not send.
9. Your online password is not working.
10. You observe unexpected software installs.
11. Your mouse moves between programs and makes selections.
12. You notice that funds are missing from your account.

WisePay has taken its website offline until the incident is remediated. It is also taking steps to implement additional security measures designed to prevent a recurrence of such an event. WisePay also has notified the UK's Information Commissioner and law enforcement to ensure the incident is properly addressed.

Please review the attachment to this letter (Steps You Can Take to Further Protect Your Information) for additional steps you can take to protect your information.

Yours sincerely,

John Coats

**Data Protection Officer  
Notre Dame High School**

### **STEPS YOU CAN TAKE TO FURTHER PROTECT YOUR INFORMATION**

#### **1. Review Your Account Statements and Notify Law Enforcement of Suspicious Activity**

As a precautionary measure, we recommend that you remain vigilant by reviewing your financial account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities.

#### **2. Copy of Credit Report**

You may obtain a free copy (30-day free trial) of your credit report from the major credit reporting agencies by visiting:

**Experian:** <http://www.experian.co.uk/>

**Equifax:** <https://www.equifax.co.uk/>

**TransUnion:** <https://www.transunion.co.uk/consumer-solutions>

#### **3. Fraud Alert**

You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least 90 days. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the credit reporting agencies identified above (as applicable).

#### **4. Security Freeze**

You may be able to put a security freeze on your credit file. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency.

#### **5. Emails**



Check if your email has been misused on [www.haveibeenpwned.com](http://www.haveibeenpwned.com)

**ONLINE**

[www.wisepay-software.com](http://www.wisepay-software.com)

**CALL**

0845 899 0011

Wise Pay Ltd is registered in England and Wales  
Registered Office: 2 Darker Street Leicester Leicestershire LE1 4SL England  
Company Reg No: 03274469 Vat No: 689397355