

# Intelligence Alert

GPMS:

OFFICIAL



OFFICIAL-SENSITIVE



Evaluation		
Source Evaluation	1	Reliable
Intelligence Evaluation	A	Known directly
Handling Code	P	Lawful sharing permitted.
National Intelligence Model Level	1: Local Issue Currently only 1 LA member affected	
Handling Conditions	Can be shared outside of the member organisation. Contents must not be uploaded to any public facing websites	

## Utility Supplier Fraud Alert

A member has reported an attempted fraud involving the supply of utilities to a school in its area. The school engaged Zenergi Limited (Zenergi), a live company that procures energy supplies and thereafter manages the supply contract. Opus Energy (Opus), also a live company who supply energy to businesses were engaged to supply gas and electricity to the school. As part of the arrangement with Zenergi, the school would have no direct contact with Opus as invoices for energy supplies would be sent via Zenergi. In spite of this, the school subsequently received a large number of telephone calls from fraudsters purporting to be Opus and claiming the school owed money. These fraudulent telephone calls culminated in a request that a direct payment arrangement be set up with Opus, failing which debt collectors would be instructed.

Fortunately, the school contacted Zenergi, who confirmed the school and Opus had been victim of an attempted fraud. They advised that the telephone number used by the fraudsters was not affiliated to Zenergi or Opus and should be blocked. The most recent call made to the school used the telephone number **01604 343 891**. Open source enquiries suggest this number is connected to an energy scam.

This appears to be part of an on-going wave of fraudulent attacks on schools. We remind all members to make educational establishments aware that they are being targeted by fraudsters and to continue to be vigilant in any dealings with third party suppliers. Any approach made purporting to be from a supplier should be independently verified using known contact details.

**If you would like to report any instances of the above information being used in similar fraud attempts please email them to [intel@nafn.gov.uk](mailto:intel@nafn.gov.uk) and the details will be forwarded to the relevant teams. Please also report to [Action Fraud](#)**

Alerts provide information about fraud, risks and trends which may affect members; your contributions are vital – please email them to [NAFN](#). Where appropriate please include handling restrictions.