

www.lancmag.com

December 2019

# Lancashire

& North West magazine

£2.45



**Santa, sleigh rides and snowballs with E. Anthony Orme**  
**Make it a Christmas to Remember with a Trip to Hayes Garden World**  
**Visit Vine Mill Furniture in Oswaldtwistle**  
**Changing the world with Rochdale Recycling**  
**A North West Lament for Europe**  
**What's the difference between an Alpaca and a Llama?**

# HOW GDPR PROTECTS FRAUDSTERS

By Andrew Harris



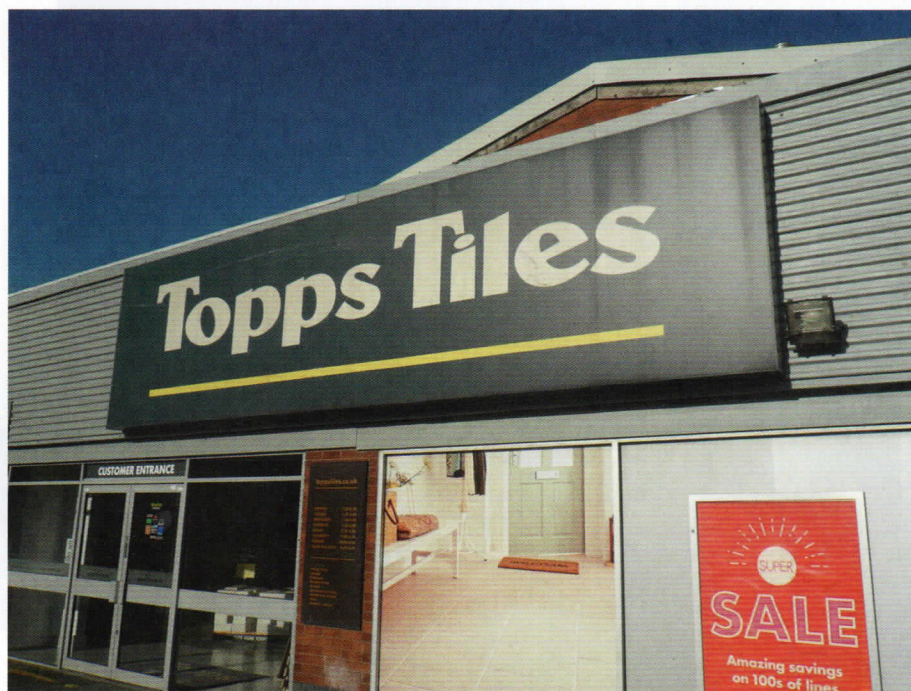
**Lloyds Bank is good with money but less good at helping to catch fraudsters.**

During the three days 12-14 March this year £1,948.47 was stolen from one of our Lloyds Bank accounts. Fortunately we keep limited funds in the current account so this took the account into overdraft and the resulting text notification from the bank alerted us to the theft. Internet information revealed that 14 payments had been made to 7 retailers. As the payments were obviously fraudulent Lloyds Bank moved swiftly and – to their great credit – the stolen sums were replaced in the account within 4 hours.

That was, however, the end of the good news. It was clear from the bank statement that the fraudster had used my card details – hacked from another source – to purchase a range of building materials including tiles, plumbing equipment, tools and something from IKEA. Courtesy of Companies House I discovered the head office contact details of all 7 companies – Topps Tiles plc, Building Materials Limited, IKEA Limited and Travis Perkins plc together with City Plumbing Supplies, Plumbnation and Toolstation which are trading names or subsidiaries of Travis Perkins and operate from their head

office address. I sent letters to all 7 on the 19th March asking them to tell me where the goods ordered online had been delivered.

Topps Tiles – which at £641.73 had received the largest single amount –



**Topps Tiles received the largest single amount and offered sympathy but no help.**

and Travis Perkins responded and said they shared my frustration but couldn't tell me where the goods ordered in my name had been delivered because of the General Data Protection Regulations or GDPR. As the goods were ordered in my name using my card details I asked them in what way was I not their customer? More sympathy followed but no information as they maintained that GDPR prevented them telling me. They might, however, be able to reveal such information to the bank or the police. IKEA and Building Materials Limited didn't bother to reply.

I contacted Lloyds Bank on the 4th April and asked them to contact Topps Tiles and Travis Perkins to ask where the goods had been delivered. The bank did not reply.

My next step was to contact Action Fraud – probably the most useless of organisations. They demanded to know the sort codes and numbers of the fraudster's bank account/s to which my funds had been transferred – thus missing the point entirely. This was an impossible request as the payments were made from my account to the retailers. Since then Action Fraud have



**Travis Perkins offered sympathy from all their companies but hid behind GDPR.**

been publicly shamed by their general behaviour. Another dead end.

My conclusion was that fraudsters can steal money with impunity because law-abiding citizens who have money taken online from their accounts cannot be told who did it or even the address to which the ordered goods were sent. Since then I have been campaigning for two reforms –

- GDPR must be changed so that people have the right to obtain full information about anything that is done in their name; and
- When retailers are selling goods or services remotely or online they must

ask the purchaser to prove that they are the cardholder.

The first reform will take longer but we now have progress with the second. The British version of EU rules which beef-up security for both online purchased and internet banking – to be called Strong Customer Authentication in the UK - will be introduced in the coming months but many responsible retailers are expected to implement the new system more quickly.

The key provision for online shopping is the introduction of an extra layer of identity checks to confound fraudsters who try to purchase goods or

services using stolen credit card details. It is expected that nearly all banks will use a mobile phone SMS text message to satisfy this extra layer of security. The way this will work is that when an online purchaser presses ‘pay’ on the retailer’s website – having already entered the stolen details – the company will send a request to the cardholder’s bank asking it to authenticate the transaction. If it is suspicious the bank will require the customer to prove that they are the owner of the card by sending a special temporary code to the mobile phone number registered under the cardholder’s name. This code is then entered on the retailer’s webpage to complete the transaction. This is likely, however, to be limited to purchases for more than £27.

Your columnist and many others have been making a thorough nuisance of themselves and, no doubt, annoying many, many fraudsters. Good! And now for GDPR which is a worthy concept but – like some health and safety rules – is often used as an excuse for avoiding doing what is legal, proper and needed.

**If you have been affected by the type of online fraud described in this article Andrew E. Harris would like to hear from you via [mail@andreweharris.co.uk](mailto:mail@andreweharris.co.uk). Your experience could help the campaign to reform GDPR. We hope to publish a further article explaining the new system of identity checks when full details are known.**



**IKEA is a big retailer but not big on replying.**