

## Retailer News – February 2015 Keeping Retailers up to date

### **Tony's Take – Economic commentary from BNZ Chief Economist Tony Alexander**

Around the world, apart from in major oil exporting countries like Russia, Venezuela and Nigeria, the question all economists and retailers are asking is this: To what extent will the downward oil price shock lead to a boost in retail spending? Theory tells us that NZ consumers, for instance, will be better off by at least \$500 a year on average. There will be some extra spending, along with extra saving. Where will the money go?

Initially we are likely to see only higher spending on small discretionary items. But as petrol prices stay low and go lower, householders will increasingly consider the decline to be permanent and they will shift their higher spending to larger items like whiteware, cars (with bigger engines) and overseas travel. This latter effect in fact could be strong given the high level of the NZ dollar which is likely to be sustained because of weakness in many other economies through this year and next.

### **Protecting your business and customers**

Merchant data breach events worryingly continue to increase both globally, as seen in some high profile compromises such as Target and Home Depot in the media, but also here in New Zealand. We have seen a significant increase in e-commerce and card-not-present merchants being targeted. The reason for this is the attacker/s undertaking this can be located anywhere in the world and do not enter the country of the merchants they are targeting.

The most easily and frequently targeted merchants are those who:

- › Use their website to collect card data, which is later manually processed.
- › Or those where the transaction is either hosted on their own system or partially hosted on their own system.

Where possible have the transaction redirected to a fully hosted solution offered by a PCI DSS compliant Service Provider.

### **What can you do?**

You can help to protect your business and customers from these data breaches by implementing the card scheme (Visa, MasterCard) endorsed Payment Card Industry Data Security Standard (PCI DSS). This is a set of standards designed to protect card data that is being processed, transmitted and stored. For more information, check out [www.bnz.co.nz/pcidss](http://www.bnz.co.nz/pcidss)

### **EFTPOS Security**

It's timely that we also remind you of the importance of checking that your EFTPOS terminal hasn't been tampered with.

### **Your EFTPOS terminal should be treated as securely as your cash register**

- › Be aware of the security around your EFTPOS terminals at all times by ensuring the terminals are left in a secure location.
- › Validate anyone claiming to be technicians.
- › Do not leave EFTPOS terminals unattended or in plain view of the public when they are not in use. If possible, secure your device to your counter.
- › Regularly check all EFTPOS terminals for signs of tampering. Record the serial numbers of your devices (Terminal and PINPad, if your PINPad is a separate component) and regularly check that the serial numbers are still the same.

### **If any of the below occur, please contact Paymark EFTPOS Helpdesk on 0800 800 996 immediately:**

- › Your EFTPOS terminal is missing.
- › You, or any member of your staff is approached to perform maintenance, swap or remove your EFTPOS terminal without prior notification from your EFTPOS provider/or security identification is not provided.
- › Your EFTPOS terminal prints incorrect receipts or has incorrect details.
- › Your EFTPOS terminal is damaged or has been tampered with.

For an online version of the recommended industry best practices, please visit [www.paymark.co.nz/eftpossecure](http://www.paymark.co.nz/eftpossecure).

If you have any queries regarding any of the above articles, or your Merchant Facility in general please contact our EFTPOS & Internet Merchant Sales and Services team on **0800 737 774, Option 4**.