Retailer News – May 2014
Keeping Retailers up to date

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

One of the key drivers of retail spending growth is consumer confidence. In that regard the portents are very good with readings at very high levels. But underlying willingness to spend still depends upon more than just feeling happy. People need to feel that it is "safe" to boost their spending. That feeling tends only to come if people feel highly confident that they will get a decent wage rise or secure more hours of work. In that regard the news is, thankfully, very positive. Employment growth has been firm for the past year and past behaviour tells us that this will very soon, if not right now, translate into faster wages growth. In addition there are many measures showing businesses are planning to strongly boost their payrolls in the near future; perhaps encouraged by the increasing difficulties they have been experiencing acquiring new staff recently. The bug-bear in all of this however is interest rates which are likely to rise by 2% - 3% over the coming two years. History tells us that high financing costs eventually curtail consumer spending. But history also tells us that this can sometimes take a long time to happen. So for the next two years we are quite confident of consumer spending showing high levels of strength which will provide retailers with some good opportunities to boost receipts, profits, get debt down, and more easily finance new lines and layouts.

Don't get hooked - beware of Phishing from online criminals

Rising use of internet for online banking, shopping and social networking increases vulnerability to scammers. Phishing is a scam that uses fraudulent emails to entice people to surrender information such as usernames, passwords and bank or credit card details. The emails are crafted to look like a legitimate email from a financial institution or a social network site and often contain links to authentic-looking but fraudulent websites. Phishing emails may contain links to websites that are infected with malicious software (malware). The rule of thumb is that a financial institution will never ask you for sensitive information via email. If in doubt, contact the institution by phone.

Criminals use online phishing scams to get your personal information, money, and identity. They send out fraudulent emails to thousands of customers every day. Many promise a tax refund to customers.

Phishing scams range from the sophisticated, convincing, and professional to those with poor English and obvious spelling and grammar mistakes.

Unfortunately, some people fall victim to these scams providing information, money, and even their identity to these online criminals.

Warning signs of a phishing attempt

If you receive an email notifying you of a tax refund or asking for your password information, here are some tips to determine if it is genuine:

- Does it include a hyperlink that asks you to submit information?
- Does it include a specific dollar value of the refund?
- Does it have errors in spelling or grammar?

If you answered "Yes" to any of those questions, delete the email from your Inbox and Trash folder.

Terminal Sunset dates for 5.2 version Terminals – 1 June 2014

This is a reminder that the 5.2 specification EFTPOS terminals are due to sunset on the 1st June 2014. This means that 5.2 EFTPOS terminals will need to be upgraded and will no longer be able to accept payments past this date.

We recommend that you discuss directly with your terminal provider about any upgrade options for your business.

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