Retailer News – April 2014
Keeping Retailers up to date

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

Employment growth in New Zealand has been strong since the middle of last year and surveys show very strong staff demand by NZ employers. Many in fact are reporting shortages. This strengthening of the labour market helps explain why consumer confidence is at a very high level and why measures of household spending are getting better. For instance the annualised pace of growth in core retail spending using debit and credit cards rose to 7.3% in the three months to February (monthly data are too volatile to use), compared with 3.8% annualised growth in the three months to November. The pace of growth has been higher in the past - over 9% in 2011 for instance - but without that pace being sustained. So one cannot blindly conclude that the path is now set toward a retailing boom - not with interest rates rising perhaps 1.5% this year. Conditions overall will certainly get better for retailers as wages growth accelerates and the unemployment rate falls potentially sharply. Plus there is a migration boom underway. But willingness of householders to borrow and spend is a lot lower than before the global financial crisis and one suspects few people will be spending their paper wealth from rising house prices. But this year should in aggregate be a good one for New Zealand retailers on average.

EFTPOS Terminal Security

It is important that merchants have heightened awareness and know what to do if they suspect their device has been stolen or compromised. Terminal tampering or skimming is the unauthorised capture of payment information. The most common approach is for fraudsters to steal a device and replace it with a compromised device which has skimming technology installed. In most cases, the fraudsters are after the information on a magnetic strip and the corresponding PIN to counterfeit cards. The fraudsters may return to collect the device or use bluetooth technology to send the data. Counterfeit spend is then often committed internationally to make purchases or withdraw cash.

Most EFTPOS terminals have in-built security features that disable the terminal if it is tampered with, however by adopting some recommended best practices you can help secure your customers' payments, protect their personal information and reduce the likelihood of credit and debit card fraud. Your business may be liable for any fines or penalties imposed by the card schemes, including forensic investigations if required, of any confirmed security breach.

Security recommendations for your EFTPOS terminal:

- 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.
- If possible, secure your device to your counter.
- Do not leave EFTPOS terminals unattended or in plain view of the public when they are not in use.
- 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 729 627 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 outline of the recommended industry best practices, please visit **www.paymark.co.nz/eftpossecure**. Paymark's website also has links to the PCI (Payment Card Industry) Security Standards Council website for further useful information.

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.**