IBM SECURITY HELPS STOP CYBERCRIMINALS FROM OPENING FRAUDULENT ACCOUNTS

New Account Fraud Technology from IBM Trusteer Protects both Consumers and Banks

Sydney - 01 Nov 2017: IBM Security today announced a new capability from IBM Trusteer that helps banks identify fraudulent accounts before they are opened. The technology also protects consumers even if they are not a customer of the bank being targeted with the fake account.

Identity fraud continues to be a global challenge, and an expensive one for banks and financial institutions. Recent estimates by the Australian Attorney-General's Department indicate that identity crime costs Australia upwards of $2.2 billion each year, with around $600 million lost through personal fraud, such as credit card fraud, identity theft and scams. According to the report, the costs of preventing and responding to identity crime are estimated to be a further $390 million, bringing the total economic impact of identity crime in Australia to approximately $2.6 billion per year. These trends are likely to continue when coupled with the historic breaches of personally identifiable information like addresses, birthdates, and more.

IBM Security helps banks and other financial service providers protect consumers by making it easier to identify fraudulent accounts with its IBM Trusteer New Account Fraud detection offering. This new technology, which is part of IBM's Trusteer Pinpoint Detect portfolio, helps financial institutions leverage machine learning to bring together the device and network information used to open a new account with analytics to help detect fraud.

IBM Trusteer New Account Fraud helps banks separate the fraudulent users from the legitimate ones, by not only looking at the positive information they provide, but comparing that with the negative indicators surrounding the transaction. The tool also looks at critical stages of the account creation process and leverages behavioral analytics to help verify identity and potential fraud patterns.

For example, details such as the IP address of where the account is being created, geolocation/time zone, and the health of the device that is being used can all be helpful in detecting fraudulent activity. If these details differ from the usual appropriate user, then it's a sign that a new account may be fraudulent.

To learn more about IBM Trusteer New Account Fraud, please visit: http://www.ibm.com/us-en/marketplace/trusteer-new-account-fraud

The New Account Fraud solution will be an add-on to IBM Security Trusteer Pinpoint Detect, which protects hundreds of global financial institutions and banking websites against account takeover and fraudulent transactions and helps detect end user machines infected with high risk malware.

About IBM Security

IBM Security offers one of the most advanced and integrated portfolios of enterprise security products and services. The portfolio, supported by world-renowned IBM X-Force® research, enables organizations to

effectively manage risk and defend against emerging threats. IBM operates one of the world's broadest security research, development and delivery organizations, monitors 35 billion security events per day in more than 130 countries, and holds more than 3,000 security patents. For more information, please visit www.ibm.com/security, follow @IBMSecurity on Twitter or visit the IBM Security Intelligence blog.

Contact(s) information

Wilma Walsh

Media relations IBM ANZ +61428 955 224wewalsh@au1.ibm.com