PwC comments on online gamers' data theft

LONDON, UK: The recent security breach which exposed millions of online gamers to risk of fraud and loss highlights yet again the need for constant vigilance on the part of anyone who uses the internet for financial transactions and on which they might also post personal information.

Commenting on the theft of 70 million online gamers' personal data in one of the largest privacy breaches to date, William Beer, a director in PwC's information security practice, said:

"The period after a breach is time-critical in terms of communicating with consumers, regulators and protecting reputation. Increasingly, consumer trust is being tested as more and more personal information is being placed in the hands of companies, but even the most respected organisations that are expected to have water-tight security are being breached as hackers become more sophisticated.

"At this point it's important that consumers are on red alert when receiving requests for their personal information. In what might seem like an authentic attempt by the company itself or a credit card supplier to rectify a problem, hackers are increasingly using advanced methods of social engineering to play on people's trust and trick them into handing over key nuggets of information.

Implications for consumers are wide-ranging

"Events like this are surrounded by uncertainty and that contributes to the severity of the problem. Targeted companies are uncertain about what has occurred and what their exposures are, while consumers are unclear about the nature of data stolen, and the motivations of the attackers. The implications of a major breach like this for consumers are wide-ranging and require increased vigilance over the months to come."

Considering the impact data breaches such as this can have on banks and credit card providers, Simon Westcott, director in PwC's financial services strategy group added:

"Since 2008, we have seen a reduction in overall credit card fraud of close to 30%, mainly due to the introduction of the chip and pin system and other online security measures. However, the nature of the threat is now changing from 'point of

sale' fraud to one perpetrated by hackers stealing large quantities of data. As more people register their credit card details across the web, the risk and cost to the credit card providers becomes ever greater.

"We expect providers to look at ways they can recover the costs of the losses they suffer and ultimately this could be passed on to consumers in the form of increased borrowing costs. We may also see providers imposing stricter security requirements on retailers and seeking to recoup some of the cost from the companies who lost the customers' data in the event these rules are not followed. Providers may also consider levying a premium for additional protection on consumers who use their credit cards online frequently."