



## FRAUD ALERT

May 5, 2011

Subject: Data Breach Announcement from Sony

United American Bank has Received the Following Announcement from the Fidelity National Information Services:

The recent statements released by Sony in regards to the data breach of personal consumer information generated many questions among our clients. The purpose of this communication is to summarize the statements released by Sony and to alert our customers of the potential phishing attacks that are likely to target affected cardholders.

Sony released the following statement on **April 28th**: "We have discovered that between April 17 and April 19, 2011, certain PlayStation Network and Qriocity service user account information was compromised in connection with an illegal and unauthorized intrusion into our network." The company says the data of some 77 million customers, including names, addresses, birthdays, passwords and log-in names, was accessed by an unauthorized person. Sony says it doesn't have evidence that credit card data was hacked, but says it "cannot rule out the possibility."

A **May 2nd** Bloomberg article stated the following: "Purchase history and credit card information may have been stolen, the company (Sony) said. The stolen data may include 10,700 direct debit records of customers in Austria, Germany, the Netherlands and Spain. The compromised debit account information included customer names, bank account numbers and account names, Sony said. The company is probing the extent of that data theft and said yesterday that it had no evidence that information on another 10 million credit cards registered to PlayStation Network and Qriocity had been leaked."

Although Sony stated only non-US card information may have been accessed, FIS Fraud Analytics proactively implemented several fraud rules to decline suspicious activity following a Sony related transaction. To date, we have not observed an increase in fraudulent activity and will continue to monitor very closely.

**We at United American Bank are closely monitoring fraud reports for any unusual activity. We would like to remind you the importance of not giving out card and personal information over the phone or via SMS or Email. More Anti-phishing information can be found at: [www.antiphishing.org](http://www.antiphishing.org)**