FOR IMMEDIATE RELEASE
April 24, 2018

Contact: Jun Chung
Community Relationship Manager
jun@jointoken.com

New Security App Generates Temporary, Secure Virtual Credit Cards

NEW YORK, NY., April 24, 2018 – Token Payments, a payment security app, makes it easy to make purchases online and over the phone without the risk of credit card numbers being stolen. All of the free-to-use security features are accessible on both Android and Apple mobile devices, and available for download right now.

In consumer trends, e-commerce is growing every year. It's expected to double between 2016 and 2020 worldwide. As more shopping moves online, so do shoppers' payment information. Account and card numbers are stored on the servers of the vendors consumers make purchases from. While this means faster and more convenient payments for the consumer, it also brings higher security risks. This is a dangerous trade-off, with retailer data breaches happening more often each year.

In just the past month, the public has been made aware of breaches at Delta Airlines, Best Buy, Under Armour, Panera Bread, Sears, Lord & Taylor, and Saks. Among the information taken in these breaches were the payment accounts associated with customers: credit and debit card numbers. How can consumers continue to confidently shop online without becoming victims of fraud?

A company called Token Payments addresses this concern by combining ease-of-use with high-end security. The Token app allows users to input their payment information onto the app, and through a process called tokenization, generate a randomized virtual credit card number that conceals the original information.

This virtual card is powered by the MasterCard network, and can be used at any online merchant. Users replace their real card numbers with payment tokens, each with a unique, temporary 16-digit card number, security code, and expiration date. Because each token only works for one vendor, any unauthorized charges made on a user's virtual card will be declined immediately. This means that during the next retailer breach, hackers will only gain access to the temporary fake number, and not the actual credit card number. The virtual cards also come with a random Cardholder name, which decreases the amount of information at risk of compromise.

Payment tokens are a game changer for payment security. Whereas a typical EMV chip-enabled credit card can tokenize account information for in-person payments, chip

support is still not widespread in the U.S., and EMV chips do absolutely nothing for online or over-the-phone payments.

The worst part of the recent retailer breaches is that they could, and should have been avoided. In an ideal world, retailers would take more measures to protect consumer financial information, or not store the information in the first place. However, saved payment methods lead to more sales from consumers, so it's unlikely that the "save card for future purchase" option is going away any time soon. That's why it's up to the consumer to protect his or her own information. Token looks to become a valuable security tool in the consumer's arsenal.