CellTrust Secure SMS Continues to be Secure, While Many Wireless Banks'Apps Were Exposed to Security Flaws

Company says Secure SMS users' information is safe and secure because of product architecture

SCOTTSDALE, ARIZONA, USA – November 22, 2010 - CellTrust Corporation, the recognized leader in mobile secure messaging and secure applications for mobile phones (www.celltrust.com), today announced that CellTrust's mobile banking product, which is being piloted outside of the U.S., is based on SecureSMS Secure Mobile information management (SMIM) architecture and is not affected by security flaws that were recently published in a Wall Street Journal article. The article stated that a number of top financial companies and banks, such as Wells Fargo & Co., Bank of America Corp. and USAA, are rushing to develop updates to fix security flaws in wireless banking applications that could allow a computer criminal syndicates to obtain sensitive data like usernames, passwords and financial information.

"This is not the first time that mobile banking applications have been vulnerable to security flaws, and we do not believe it will be the last time," said Sean Moshir, CEO and Chairman of CellTrust. "The issue with the banking apps mentioned in The Wall Street Journal article is that personal information about the wireless subscriber, such as the user name and password to a bank account, is being stored in the mobile device, which could give a cybercriminal full access to a person's financial accounts. Storing the password in the memory of the handset is a fundamental mistake in the design of the apps and the security architecture. Furthermore, apps that store passwords in the memory of the handset or send it across the network are not compliant with financial industry regulations or best practices."

Moshir continued, "CellTrust developed its SecureSMS platform from the ground-up, with security architecture in mind, and continues to provide a safe and secure environment for the exchange of sensitive information. A key difference with SecureSMS is that CellTrust uses the mobile command channel for communication, rather than the data channel which was used for

these particular mobile banking apps. It is critical and added security for mobile banks apps to perform the actual transaction or user authentication out of band."

CellTrust SecureSMS provides:

- Two-factor authentication
- End-to-end encryption of messages
- Long SMS messages, of up to 5000 characters
- Confirm delivery and read receipt
- Policy-based encryption key changes
- Auditing and compliance with HIPAA, FISMA, and Sarbanes-Oxley, ensuring that information is kept private and only delivered to the intended recipient
- Remote data wipe if a device is lost or unauthorized access attempts are detected
- Architecture that does not store passwords in the memory of handset or transmit it across the wireless network

CellTrust SecureSMS™ Appliance was named winner of many industry awards by CTIA, Mobile Marketing Association, RCR Magazine, MobileTrax, and more.

About CellTrust Corporation
CellTrust is a leading provider of secure mobile messaging and applications. CellTrust's patent pending SecureSMS Gateway™ featuring the SecureSMS™ Appliance and a suite of mobile applications provide advanced secure mobile messaging and information management across 200+ countries and over 800 carriers. CellTrust ensures the secure and trusted exchange of information on mobile devices to the financial services, healthcare, government, education, energy, information technology, marketing, and travel, among other global industries. For more information about CellTrust's Global, African, North American and Australian operations: www.celltrust.com www.africa.celltrust.com www.celltrust.com.au

# # #

Media Contact:
Lora Friedrichsen
Global Results Comms (GRC) for CellTrust
+1 949-608-0276
celltrust@globalresultspr.com