FOR IMMEDIATE RELEASE

New Zeus Trojan Variant Puts Consumers at Risk -- CellTrust Secure SMS Continues to be Safe and Secure for Mobile Banking

SecureSMS users' information is safe and secure because of CellTrust's secure product architecture

SCOTTSDALE, ARIZONA, USA – March 1, 2011 - 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 products based on SecureSMS Secure Mobile information management (SMIM) architecture are not affected by the new Zeus Trojan, exposed in an alert by F-Secure. The article described how the new Zeus variant, "Mitmo," affected the ING bank in Poland by stealing mTANs from customers, mobile authentication numbers sent by SMS that enable online transactions. Mitmo offered mobile users an altered version of the bank's website accessible by the user's login, password, phone model and number. Once admitted, the user is sent an SMS linked to a corruptible application, which collects data that can be used to wipe out a bank account.

"The Zeus Trojan that targeted the ING Bank in Poland is similar to the one that targeted Spain last year, showing that mobile security continues to put consumers at significant risk," said Sean Moshir, CEO and Chairman of CellTrust. "Passing along personal information, such as the user name and password to a bank account, through a mobile device gives a cybercriminal easy access to a person's financial accounts. Most security programs that send personal information 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 SecureSMS messages are authenticated with source and destination verified using an

encryption key that changes based on policy. It also detects if the content or the payload of the SMS has been tampered with."

Other key factors of the SecureSMS architecture lie in the unique communication key, specific to each client mobile device and the transmission of information through the secure gateway appliance. These elements provide a degree of security above and beyond any standard encryption based products that have ever been proposed within the market to date.

Operators worldwide are searching for solutions to help protect their wireless subscribers from security risks, such as the Zeus Trojan. Recently, Celcom, the largest 3G operator in Malaysia (http://www.celcom.com.my), launched the CellTrust SecureSMS Consumer app for the BlackBerry operating system, now available for download by Celcom's wireless subscribers on the BlackBerry app store. Additionally, Celcom has made the CellTrust SecureSMS Enterprise appliance model available to its corporate, government and other enterprise customers featuring either a dedicated or hosted server option, which can be integrated into their own enterprise infrastructure.

CellTrust's SecureSMS is offered either as a Cloud Service for carriers, enterprise, or consumers, or in a customer administered Gateway Appliance configuration. The Secure Gateway Appliance comes preconfigured, with APIs provided, allowing for ease of incorporation into existing infrastructure and operations. CellTrust forged this development model to design a true turnkey solution that resolves both industry and consumer need for security measures, and implementation issues that had hampered previous provider attempts. This is a real final solution; one that actually addresses every issue, and solves the problem at hand.

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/Valerie Christopherson
Global Results Comms (GRC) for CellTrust
+1 949-608-0276
celltrust@globalresultspr.com