

**Fraudulent Electronic Funds Transfers (EFT)  
August 26, 2009**

The Federal Deposit Insurance Corporation (FDIC) has alerted us of an increased number of fraudulent EFT transactions originated by unknown individuals who have compromised legitimate business computer systems. As the result of these compromises unauthorized EFT's, such as automated clearing house (ACH) and wire transfers have been created. Most often the business customer is unaware of the fraudulent activity until a review of their account is performed.

Typically a computer is infected by trickery, they produce a prompt on-screen that appears to be a warning from the user's computer, anti-virus program or e-mail with an attachment and if the user clicks on the program it infects the system.

In order to avoid these types of losses businesses and local government agencies can find cyber security resources at <http://www.us-cert.gov/>. You can also speak with a bank representative who will be able to assist you.

\*\*\*\*\*

**Special Alert**

SA-147-2009  
August 26, 2009

TO: CHIEF EXECUTIVE OFFICER  
SUBJECT: Fraudulent Electronic Funds Transfers (EFTs)  
Summary: *The Federal Deposit Insurance Corporation is aware of an increased number of fraudulent EFT transactions resulting from compromised login credentials.*

The Federal Deposit Insurance Corporation (FDIC) is alerting financial institutions that provide Web-based payment origination services for business customers to increased reports of fraudulent EFT transactions resulting from compromised login credentials. Over the past year, the FDIC has detected an increase in the number of reports and the amount of losses resulting from unauthorized EFTs, such as automated clearing house (ACH) and wire transfers. In most of these cases, the fraudulent transfers were made from business customers whose online business banking software credentials were compromised.

Web-based commercial EFT origination applications are being targeted by malicious software, including Trojan horse programs, key loggers and other spoofing techniques, designed to circumvent online authentication methods. Illicitly obtained credentials can be used to initiate fraudulent ACH transactions and wire transfers, and take over commercial accounts. These types of malicious code, or "crimeware," can infect business customers' computers when the customer is visiting a Web site or opening an e-mail attachment. Some types of crimeware are difficult to detect because of how they are installed and because they can lie dormant until the targeted online banking session login is initiated. These attacks could result in monetary losses to financial institutions and their business customers if not detected quickly.