Federal Deposit Insurance Corporation
550 17th Street NW, Washington, D.C. 20429-9990

Financial Institution Letter
FIL-37-2016
June 7, 2016

FFIEC Joint Statement on Cybersecurity of Interbank Messaging and Wholesale Payment Networks

Summary: The FDIC, as a member of the Federal Financial Institutions Examination Council (FFIEC), is issuing the attached statement advising financial institutions to actively manage the risks associated with interbank messaging and wholesale payment networks.

Statement of Applicability to Institutions with Less than $1 Billion in Total Assets: This Financial Institution Letter (FIL) applies to all FDIC-supervised institutions**.**

Suggested Distribution:
FDIC-Supervised Banks (Commercial and Savings)

Suggested Routing:
Chief Executive Officer
Chief Information Office
Chief Information Security Officer

Attachment:
FFIEC Joint Statement on Cybersecurity of Interbank Messaging and Wholesale Payment Networks

Related Topics:
FFIEC IT Examination Handbook

Contact:
Donald Saxinger, Senior Examination Specialist, at dsaxinger@fdic.gov or (703) 254-0214

Marlene Roberts, Senior Specialist Critical Infrastructure Protection at MarRoberts@fdic.gov or (703) 254-0465

Note:
FDIC Financial Institution Letters (FILs) may be accessed from the FDIC's Web site at https://www.fdic.gov/news/news/financial/2016/.

To receive FILs electronically, please visit http://www.fdic.gov/about/subscriptions/fil.html.

Paper copies may be obtained through the FDIC's Public Information Center, 3501 Fairfax Drive, E-1002, Arlington, VA 22226 (1-877-275-3342 or 703-562-2200).

Highlights:

- Recent cyberattacks have targeted interbank messaging and wholesale payment networks, resulting in large-dollar fraud at several foreign institutions. These attacks have demonstrated a capability to:
  - Compromise the financial institution's wholesale payment origination environment and bypass information security controls;
  - Obtain and use valid operator credentials to create, approve and submit messages;
  - Employ a sophisticated understanding of funds transfer operations and operational controls;
  - Use highly customized malware to disable security logging and reporting, as well as other operational controls, to conceal and delay the detection of fraudulent transactions; and
  - Quickly transfer stolen funds across multiple jurisdictions to avoid recovery.
- Financial institutions should conduct a risk assessment to determine whether effective risk-management practices and controls are in place. Institutions should consult their payment system provider's guidance for specific security control recommendations.
- Additional information on cybersecurity and wholesale payment systems can be found in the following FFIEC IT Examination Booklets:
  - Information Security
  - Wholesale Payment Systems