nonbanking company complies with the standards in section 4 of the BHC Act (12 U.S.C. 1843). Unless otherwise noted, nonbanking activities will be conducted throughout the United States.

Unless otherwise noted, comments regarding each of these applications must be received at the Reserve Bank indicated or the offices of the Board of Governors not later than January 27, 2017.

A. Federal Reserve Bank of St. Louis (David L. Hubbard, Senior Manager) P.O. Box 442, St. Louis, Missouri 63166–2034. Comments can also be sent electronically to *Comments.applications@stls.frb.org:*

1. *American Pacific Bancorp, Inc.,* Harrisburg, Illinois; to become a bank holding company by acquiring 67 percent of Main Street Bancshares, Inc., Harrisburg, Illinois, and thereby indirectly acquiring Grand Rivers Community Bank, Grand Chain, Illinois.

Board of Governors of the Federal Reserve System, December 29, 2016.

Yao-Chin Chao,

Assistant Secretary of the Board.

[FR Doc. 2016–31913 Filed 1–3–17; 8:45 am]

BILLING CODE 6210–01–P

FEDERAL RESERVE SYSTEM

Change in Bank Control Notices; Acquisitions of Shares of a Bank or Bank Holding Company

The notificants listed below have applied under the Change in Bank Control Act (12 U.S.C. 1817(j)) and § 225.41 of the Board's Regulation Y (12 CFR 225.41) to acquire shares of a bank or bank holding company. The factors that are considered in acting on the notices are set forth in paragraph 7 of the Act (12 U.S.C. 1817(j)(7)).

The notices are available for immediate inspection at the Federal Reserve Bank indicated. The notices also will be available for inspection at the offices of the Board of Governors. Interested persons may express their views in writing to the Reserve Bank indicated for that notice or to the offices of the Board of Governors. Comments must be received not later than January 18, 2017.

A. Federal Reserve Bank of Kansas City (Dennis Denney, Assistant Vice President) 1 Memorial Drive, Kansas City, Missouri 64198–0001:

1. *The Bryant James Gingrich 2012 Irrevocable Trust, the Bryant James Gingrich 2016 Irrevocable Trust, and Bryant James Gingrich, acting in his capacity as trustee of both trusts,* all of Alva, Oklahoma; *the Chad Wisdom McManus 2012 Irrevocable Trust, the Chad Wisdom McManus 2016 Irrevocable Trust, and Chad Wisdom McManus, acting in his capacity as trustee of both trusts,* all of Enid, Oklahoma; *and the Kelsey Grace Gingrich 2012 Irrevocable Trust, the Kelsey Grace Hunter 2016 Irrevocable Trust, and Kelsey Grace Hunter (née Gingrich), acting in her capacity as trustee of both trusts,* all of Edmond, Oklahoma; to acquire voting shares of Grace Investment Company, Inc., Alva, Oklahoma, and thereby join the existing Peggy J. Wisdom Family Control Group previously approved to control 25 percent or more of the voting shares of Grace Investment Company, Inc. Grace Investment Company, Inc. is the parent holding company of Alva State Bank and Trust Company, Alva, Oklahoma; First National Bank in Okeene, Okeene, Oklahoma; and The First State Bank, Kiowa, Kansas.

Board of Governors of the Federal Reserve System, December 29, 2016.

Yao-Chin Chao,

Assistant Secretary of the Board.

[FR Doc. 2016–31914 Filed 1–3–17; 8:45 am]

BILLING CODE 6210–01–P

FEDERAL TRADE COMMISSION

IoT Home Inspector Challenge

AGENCY: Federal Trade Commission.

ACTION: Notice; public challenge.

SUMMARY: The Federal Trade Commission (''FTC'') announces a prize competition that challenges the public to create a technical solution (''tool'') that consumers can deploy to guard against security vulnerabilities in software on the Internet of Things (''IoT'') devices in their homes. The tool would, at a minimum, help protect consumers from security vulnerabilities caused by out-of-date software. Contestants have the option of adding features, such as those that would address hard-coded, factory default or easy-to-guess passwords. The prize for the competition is up to $25,000, with $3,000 available for each honorable mention winner(s). Winners will be announced on or about July 27, 2017.

DATES: The deadline for registering and submitting entries is May 22, 2017 at 12:00 p.m. EDT. Further instructions and requirements regarding the registration and submission process will be provided on the Contest Web site (*ftc.gov/iothomeinspector*).

FOR FURTHER INFORMATION CONTACT: Ruth Yodaiken, 202–326–2127, Division of Privacy and Identity Protection, Bureau of Consumer Protection, FTC; 600 Pennsylvania Ave. NW., Mailstop CC–8232, Washington, DC 20580.

SUPPLEMENTARY INFORMATION: The FTC IoT Home Inspector Challenge (the ''Contest'') encourages the public to create a tool that consumers can deploy to guard against security vulnerabilities in software on the IoT devices in their homes. The tool would, at a minimum, help protect consumers from security vulnerabilities caused by out–of-date software. The competition's purpose is to stimulate innovation and progress in protecting and empowering consumers against security risks associated with IoT devices in the home.

A. Background

Every day, American consumers use Internet-connected devices [1] to make their homes ''smarter.'' Consumers can remotely program their smart home devices to turn on their lights, start the oven, and turn on soft music so they return to a comfortable environment when they get home from work. Smart video monitors enable consumers to remotely view their homes, pets, or children. Smart fire and burglar alarms address safety issues through sensors and alerts. And smart thermostats can automatically adjust temperature settings depending on the time of day and presence of people in the house. To tie all these devices together, smart home platforms are also beginning to proliferate across the marketplace.

While these smart devices enable enormous convenience and safety benefits, they can also create security risks. For example, press reports from October 2016 demonstrated how smart devices could be used in ''botnets'' to disrupt the Internet.[2] This incident demonstrated that lax IoT device security can threaten not just device owners, but the entire Internet. In another incident, a group of hackers allegedly gained unauthorized access to routers manufactured by the tech company ASUS and left a text file warning stating, ''Your Asus router (and your documents) can be accessed by anyone in the world with an internet connection.'' [3] The FTC announced a

[1] As used herein, ''Internet-connected,'' ''IoT,'' or ''smart'' devices are devices other than desktop or laptop computers or smartphones.

[2] *See, e.g.,* ''Americans uneasy with IoT devices like those used in Dyn DDoS attack, survey finds,'' Tech Crunch, Darrell Etherington (October 24, 2016) (stating that a ''coordinated botnet attack effectively choked internet access to a large number of popular sites'' and was attributed ''in large part due to the spread of connected Internet of Things (IoT) devices''), *available at https://techcrunch.com/2016/10/24/americans-uneasy-with-iot-devices-like-those-used-in-dyn-ddos-attack-survey-finds/.*

[3] ''ASUS Settles FTC Charges That Insecure Home Routers and ''Cloud'' Services Put Consumers'