Florida Baptist board hears update on financial fraud

August 30, 2023

JACKSONVILLE, Fla. (BP)—Florida Baptists' State Board of Missions heard a report from the subcommittee tasked with providing oversight and recommendations regarding the investigation into financial fraud discovered by the Florida Baptist Convention in May.

Subcommittee members—Aaron Burgner, Darren Gaddis, Paul Purvis, Brian Stowe and Angel Turbeville—worked with federal and state investigators, internal and external auditors and cyber forensics experts in their investigation into the more than $700,000 in funds stolen from the convention through cybertargeting.

The investigation revealed no criminal activity on the part of any Florida Baptist Convention staff person but instead concluded that the crime was the result of sophisticated cybertargeting by—at this point—unknown perpetrators.

The subcommittee's work culminated in the recommendation for strengthened financial protocols and ongoing training for convention staff.

To prevent such a crime from occurring in the future, the convention is exercising heightened awareness when carrying out financial duties, implementing appropriate data security controls, and completing the process to become accredited by the Evangelical Council for Financial Accountability. The convention still is making efforts to recover the stolen funds.

Florida Baptist Convention Executive Director-Treasurer Tommy Green acknowledged this is the first time he has dealt with a crime of this nature

in his more than four decades of ministry.

“Everything we do is built on trust,” he said. “I’m sorry. We will move forward. We are better, and we’ll continue to get better.”

He has already seen, he said, that “churches are learning from the convention’s fraudulent experience.”

The convention recommends these best practices to help churches protect their financial assets:

- Provide staff training on recognizing suspicious emails and other sophisticated cyberattacks.
- Enable multifactor authentication logins when available.
- Verbally verify any changes to payment instructions requested by a vendor related to accounts payable or an employee related to payroll.
- Discuss with the church’s insurance agent the programs and levels of coverage available to help the church in the event of a cyberfraud experience.
- Engage a cybersecurity professional to provide analysis of information technology infrastructure and security.