

Cyberfraud costs Florida Baptists more than \$700,000

May 17, 2023

WASHINGTON (RNS)—Staff at the Florida Baptist Convention thought they were sending mission money to help pay for church planting. Then the money disappeared.

“The Florida Baptist Convention continues to work with federal and state investigators, our internal and external auditors to recover over \$700,000 in funds stolen from the convention through cyber-targeting,” according to a May 15 update on the convention’s website.

Florida Baptist officials first announced they’d been a victim of fraud on Wednesday but had not shared the scope of the loss. The announcement on the convention’s website was updated after Religion News Service asked leaders at the convention to confirm the size of the loss.

The Florida Baptists are one of more than 40 state conventions affiliated with the Southern Baptist Convention. The funds were meant to go to the SBC North American Mission Board, which partners with the Florida Baptists in church planting.

That process was interrupted when the Florida Baptist staff received an email that claimed to be from NAMB but was not and requested funds be sent to a new account number. The fraudulent email reflected “a general knowledge of the communications and practice between the SBC entity and the convention.”

“An investigation is being launched to determine how this knowledge was gained,” the convention said in a statement informing its supporters. “At this time, we have no reason to suspect malfeasance by any convention

employees.”

Convention leaders said they will honor their commitments to support churches and other ministries despite the loss by drawing on reserves. They also said they would add to their cybersecurity, which according to leaders already included “training, regular information systems upgrades, and advanced detection software.”

Warning against cybercrimes

They also warned churches about the ongoing danger of cybercrimes.

“These types of attacks continue to plague organizations of all sizes and scopes,” the convention said in a statement. “We encourage pastors and churches to remain diligent with the security of their IT and financial systems. This specifically includes critically scrutinizing any and all requests—even those from a supposedly well-known source—that request a shift from historical payment practices.”

Mike Ebert, a spokesman for NAMB, said that agency adheres to “robust cyber and data security protocols, follows best-in-class accounting principles and internal controls” to protect donations from Southern Baptists.

“We have and will continue to support our ministry partners as they seek to do the same,” Ebert said in a text message.

Earlier this year, a church in North Carolina reportedly lost close to \$800,000 after receiving a fraudulent email. Johnny Blevins, pastor of Elkin Valley Baptist Church, told a North Carolina television station the church received an emailed bill from a contractor working on the church building.

“Immediately following that email was another email, which we thought was from Landmark,” Blevins told the television station. “It had cloned

basically that email and it gave instructions on payment and included the invoice and everything.”

The fraud was reportedly discovered when the contractor called, asking about the unpaid bill. A GoFundMe campaign to replace some of the North Carolina church losses has raised \$7,761, far short of the \$793,848 goal.

Recovering any funds likely will be a drawn-out process, as the United Church of Marco Island, a Florida Gulf Coast congregation, has discovered. The church lost \$1.2 million to fraud in March 2022.

About half of the money was recovered, but the church’s insurance company declined to cover any of the church’s losses, saying the church policy did not cover “impersonation fraud,” according to a complaint against the insurer filed by the church in state court. The case was recently moved to a federal court in Florida.

Be wary when it comes to finances

John Hughes III, the attorney who represents the church, declined to discuss the specifics of how the fraud occurred. But he did say many of the cases of cyberfraud affecting churches are similar—often involving fake phishing emails. Those emails are often created, he said, by taking a real email and cutting and pasting its contents, including email signatures.

Hughes warned that churches and businesses need to be wary because of the relentless efforts of fraudsters. Especially when it comes to finances.

“Any instructions that come by email—they need to confirm them via phone call,” he said. Otherwise, he added, “they just wire the money out and it’s gone.”

He especially warned of the need for care in dealing with familiar financial transactions—where people might be tempted to click send without reading

the entire email.

Hughes also suggested churches and other groups be proactive in talking to their insurance company about fraud. He argued that in the case of the Marco Island church, the loss should be covered. But the process of recovering losses, he said, will be long.

The church's insurance company did not respond to a request for comment.

Florida Baptists hope that some of the losses will be recovered.

"We remain prayerful that some of this loss may be mitigated through insurance and/or the recovery of stolen funds," the convention's update states.