TETON
SCHOOL DISTRICT 401
EMPOWERING OUR STUDENTS TO REALIZE THEIR FULL POTENTIAL
PO Box 775 Driggs, ID 83422
Ph: 208 228 5923 Fax: 208 354 2250

Monte R. Woolstenhulme, Ed. S
Superintendent

FRAUD INCIDENT SUMMARY UPDATE

July 24, 2019

Sept. 16, 2019 School Board adoption

The purpose of this document is to summarize the fraud incident that occurred Dec. 20, 2018, in Teton School District 401. This is a revision to the document dated June 3, 2019. Links are provided to relevant documents.

Part 1: A summary of the school district's action, and the various organizations that assisted with this incident will be noted:

A. Summary of Events:

- On December 20, 2018, Superintendent of Schools Monte Woolstenhulme discovered that Teton School District 401 was the victim of an email phishing scam. As a result of the scam, a TSD 401 building construction payment of $784,000 was transferred electronically to a fraudulent bank account.
- Superintendent Woolstenhulme contacted the Teton County Sheriff's Office and federal law enforcement (FBI) immediately opened an investigation of the incident.
- Within two weeks, the FBI located $484,332.66 of the stolen funds in an out-of-state bank account. These funds were returned to TSD 401 on January 10, 2019.
- TSD's insurer (ICRIMP) covered the remainder of the loss, plus some of the expense for district cybersecurity training, in the amount of $300,051.05. These funds were received by TSD 401 on February 13, 2019.
- Between the partial recovery of stolen funds and the coverage of the remainder by insurance, the school district was made financially whole within 60 days of the original incident.
- The FBI has not commented to date on the 2018 incident, to TSD 401 or local law enforcement about the case. The FBI has stated that it does not release information or make public statements about such cases.

- The school building construction payments have continued according to plan with no interruption to schedule. The bond-supported school buildings are on track to be completed according to the construction schedule.
- The initial loss was the result of a single TSD 401 employee not following established protocol for making such payments. A request by that employee to the bank to increase the allowable transfer amounts occurred with the bank. That employee has been dismissed and a replacement employee hired.
- Although adherence to previously in-force protocols would have prevented the fraud, the school board strengthened district financial protocols. Cybersecurity training for staff continues.
- Direct communication with the bank and others on construction payments occurs regularly to ensure accuracy and verification of monthly payments.

B. Organizations that assisted with the fraud incident:

1) Law Enforcement: Teton County Sheriff's Department, Deputy Andy Sewell as lead investigator (Driggs); *no summary report provided to the school district, however, information was shared with the local newspaper.*

2) Law Enforcement: Federal Bureau of Investigation (FBI), Special Agent Bodily, (Pocatello Field Office), lead investigator; *no summary report provided.*

3) Bank of Commerce, Aaron Hanson, (Driggs local branch manager), Carlan McDaniel, COO, (Idaho Falls Main Office); *see attached summary letter.*

4) Idaho Counties Risk Management Program (ICRMP) (TSD Insurance carrier), Jeff Boice, lead claims specialist (Boise), Craig Chandler, local insurance agent (St. Anthony); *see attached summary letter*, and *closing verification letter.*

5) Attorney: D. Andrew Rawlings, Holden Kidwell Hahn & Crapo, attorneys, (Idaho Falls), school district legal counsel; *see attached summary letter.*

6) Financial Auditors, Rudd & Company, Scott Bond, lead auditor (Idaho Falls); see *attached summary letter.*

7) Regional School District Business Manager assistance, Varr Snedaker, Madison School District 321 Business Manager, assisted school district finances, (Rexburg) January-April, 2019.

8) Headwaters Construction, Bryer Hastings, Project Manager, direct lead for all matters on school construction projects; *see attached summary letter.*

Part 2: A timeline of events, listing of school board meetings, actions taken, and reference materials will be noted:

A. Fraud incident timeline:
- Dec. 20, 2018: Notification of Headwaters inquiring about the December fraud email; superintendent notified law enforcement of fraudulent email; initiated school district investigation.
- Dec. 21, 2018: continued school district investigation, placed business manager on administrative leave, accepted his resignation.
- Dec. 28, 2018: special school board meeting (executive session).
- Jan. 7, 2019: notification from the Bank of Commerce, through the FBI investigation, that approximately $484,000 of the original funds have been recovered (announced to the public at session school board session).
- Jan. 10, 2019: confirmation that $484,332.66 of the original funds have been deposited into the school district Bank of Commerce account.
- Feb. 13, 2019: confirmation the insurance company, ICRMP, will cover the remaining loss of funds and some cyber-security training expenses: $300,051.05, less a $500 deductible, paid by TSD401.
- Ongoing:
  - Cybersecurity training for financial, administrative and all school staff, through the school district IT staff.
  - Increased security protocol regarding all financial invoices, and specifically construction related invoices, payments, and authorized disbursement of those payments to approved contractor representatives, and verification funds have been received.
  - Additional training and communication steps with school district financial staff, administration, school board representative and contractors regarding all invoices and payments.

B. School Board Meetings

- Special Board meeting: Dec. 28, 2018 (executive session)
- Special Board meeting: Jan. 7, 2019 (special session)
- School Board meeting: Jan. 14, 2019 (regular monthly meeting)
- Special Board meeting: Feb 4, 2019 (executive session)
- School Board meeting: Feb. 11, 2019 (regular monthly meeting)

C. Actions taken by the school district:

a. Staffing: replacement of school district business manager.

b. Enhanced security procedures regarding all construction invoices, payments and verification of payments received by contractors.

c. Cooperated with Law Enforcement (Teton County Sheriff's Department, FBI).

d. Carried out cybersecurity training with TSD401 IT Staff and all district personnel.

e. Communicating with contractors, architects, school board designee and school district financial staff on all payments and communication regarding payments.

f. Responded to the following Public Records Requests (PRR) that relate to this fraud incident:

1. For all written communication between TSD401 and the FBI
2. Phone records of calls to FBI
3. Emails from 2018 regarding Headwaters request for electronic payments

D. Reference items:

- Press Release updates sent by the school district to local and regional media that relate to the fraud incident:
  - December 28, 2018
  - January 8, 2019
  - January 10, 2019
  - January 15, 2019
  - February 13, 2019
- Letter to the editor, emailed to *Teton Valley News* (December 22, 2018) and to David Plourde of KIFI Channel 8 (December 26, 2018)
- List of Frequently Asked Questions, distributed to the public at special session of school board (January 7, 2019)
- Moody's Investor Services Cybersecurity review (references TSD 401 incident)
- Cybersecurity Incidents in the USA (April 2019 Techlearning.com article)

Summary report prepared by:
Monte R. Woolstenhulme, Ed. S., Superintendent
Teton School District 401

Reviewed by:
Jeanne Anderson, PR Consultant, Teton School District 401