



DICKINSON PUBLIC SCHOOLS INCIDENT REVEALS CRITICAL VENDOR PAYMENT PROCESS GAPS

In February 2026, Dickinson Public Schools in Dickinson, ND, experienced a significant Business Email Compromise (BEC) incident. **This breach exposed vulnerabilities in their vendor payment processes, resulting in a substantial financial loss.**

This incident underscores the importance of robust process controls to protect district funds from similar attacks. Business Email Compromise, a form of cybercrime where attackers impersonate legitimate business contacts to redirect payments, continues to be a prevalent threat. According to the FBI's Internet Crime Report (2024), BEC scams accounted for over \$2.4 billion in losses in 2023 alone. This article explores key process controls that districts can implement to safeguard their financial operations.

CALLBACK VERIFICATION

Callback verification is a critical control measure that involves confirming payment requests through a secondary communication channel. This process ensures that any changes to vendor payment details are legitimate. For instance, if a vendor emails a change to their bank account information, finance staff should call the vendor using a known phone number to verify the request. This step is crucial in preventing unauthorized changes that could redirect funds to fraudulent accounts. Implementing callback verification can significantly reduce the risk of BEC incidents affecting district operating funds and payroll accounts.

DUAL AUTHORIZATION

Dual authorization requires two separate individuals to approve significant financial transactions. This control adds an additional layer of oversight, making it more difficult for fraudulent transactions to go unnoticed. In the context of a school district, this might involve a finance officer and a superintendent both reviewing and approving vendor payments. By requiring dual authorization, districts can ensure that no single point of failure exists in their payment processes, thereby protecting restricted capital accounts and construction project payments.

OUT-OF-BAND CONFIRMATION FOR ACH CHANGES

Out-of-band confirmation involves verifying changes to Automated Clearing House (ACH) payment instructions through a different communication channel than the one used to request the change. For example, if a vendor emails a request to change their ACH details, the district should confirm this change via a phone call or a secure messaging platform. This practice helps verify the authenticity of the request and prevents unauthorized account changes. Implementing out-of-band confirmation can safeguard district funds from being misdirected due to fraudulent instructions.

FAST REPORTING TO THE FBI

Promptly reporting BEC incidents to the FBI can improve the chances of recovering lost funds. The FBI's Recovery Asset Team works to freeze and recover funds that have been fraudulently transferred. According to the FBI's Internet Crime Report (2024), quick reporting significantly enhances the likelihood of successful fund recovery. Districts should establish a protocol for immediate reporting of suspected BEC incidents to maximize recovery efforts and minimize financial losses.

OPERATIONAL CONSEQUENCES

The operational consequences of failing to implement these controls can be severe. Without proper verification processes, districts risk losing substantial amounts of money, which can impact their ability to fund essential services and projects. Moreover, the loss of community trust and potential reputational damage can have long-lasting effects. By adopting these process controls, districts can protect their financial resources and maintain the trust of their stakeholders.

In conclusion, the Dickinson Public Schools incident serves as a stark reminder of the vulnerabilities present in vendor payment processes. By implementing callback verification, dual authorization, and out-of-band confirmation, districts can significantly reduce their risk of falling victim to BEC scams. Prompt reporting to the FBI further enhances the chances of recovering lost funds. These measures are not just theoretical recommendations but practical steps that can be implemented this quarter to safeguard district finances.

To further strengthen your organization's cyber defenses, visit our [Cyber Awareness Training](#) page to learn how ongoing employee training helps prevent phishing, Business Email Compromise (BEC), and other cyber threats.

SECURE YOUR SCHOOL DISTRICT OR COMMUNITY COLLEGE WITH A FREE CYBER READINESS CHECK & INCIDENT RESPONSE PLAN

