Preventing State and Local Government Payments Fraud

KYRIBA FACT SHEET

State and local government entities, as well as governmental agencies across the country, are experiencing a drastic increase in payments fraud, which has resulted in millions of dollars in losses. For government offices looking to streamline their payments, prevent fraud and stay out of headlines, the need for a robust cybersecurity strategy is imperative. Government entities at all levels must realize without adequate payment fraud controls, banks and cybersecurity insurance may not cover losses and related litigation.

Governments who are experiencing payments fraud are seeing a number of different deception tactics from cybercriminals to gain access to their liquidity. Often posing as an internal employee or an external vendor, fraudsters are deploying threats such as:

Social Engineering

The use of deception to manipulate individuals into divulging confidential or personal information that may be used for fraudulent purposes.

Impersonation

Fraudulent cybercriminal(s) pretending to be a vendor, manager or executive to make a payment request or to change banking instructions.

Business Email Compromise (BEC):

A request made via email to send, change or update payment instructions.

Deepfake

When a cybercriminal uses video, photo, audio or voice to alter their identity and impersonate a company employee to send payments.

Kyriba provides governmental agencies with the ability to centralize and detect potential fraud in real time, stopping suspicious payments in their tracks.

Public sector treasury departments have a lot at stake when a payments fraud attempt is successful. From the loss of funds to reputational risk and unfavorable press to banks viewing them as high-risk clients, fraud can do massive damage to a government agency. Furthermore, organizations don't have as much protection as they might think. Banks are under no obligation to cover any client losses unless the bank itself was breached. And cyber insurance doesn't always cover payments fraud, as some recent cases have shown.

As for technology, treasury and accounts payable teams often do not have end-to-end fraud prevention tools in place to standardize their payments policies and procedures. When building payment workflows, it is important to consider how internal processes will actively work to mitigate payments fraud and fraudulent invoicing to prevent examples of payment control breakdowns that lead to fraud like the following:

County In North Carolina lost $4M + due to a BEC fraud scam

The cybercriminal mimicked the email address of a county contractor, but with extra hyphens in the domain name.

Texas school district lost $2.3M due to a phishing scam

The cybercriminal launched a fraudulent email campaign, leading to three separate fraudulent transactions.

As cybercriminals continue to target government entities with seemingly high success rates of payments fraud, organizations should look to leverage robust, end-to-end payment and fraud prevention modules to automate and solidify their payments fraud strategy.

Kyriba provides governmental agencies the ability to centralize and detect potential fraud in real time, stopping suspicious payments in their tracks. The module utilizes a rule-based, machine learning model to comply with internal policies, and provide alerts and anti-fraud controls for users to immediately detect possible fraudulent payments for investigation, based on identified anomalies compared to payment history and fraud patterns.

For more insights
Visit Kyriba's public sector or payments page