CASE STUDY

Industry: **Real estate developer, owner and investor**

Solutions: **Kyriba Enterprise**
- **Cash**
- **Cash Forecasting**
- **Debt & Investments**
- **GL Post**
- **In House Bank**
- **Payments**

Combatting Fraud – Treasury Real World Experiences

Companies are increasingly being targeted by fraud attacks – and the techniques used by fraudsters are becoming ever more sophisticated.

In the 2016 AFP Payments Fraud and Control Survey, the statistics show an increase across payments, wire fraud and business email compromise (BEC) fraud attempts:

- **73%** of companies were targets of payments fraud in 2015 (meaning they experienced attempted and/or actual payments fraud*.
- **48%** of organizations were exposed to wire fraud in 2015 – a huge increase from the 27% of organizations who were exposed in 2014*.
- Business email compromise (BEC) scams, where criminals imitate a CEO or CFO and use email communication to deceive employees into making payments into fraudulent accounts, are believed to be responsible for the increase in overall payments fraud activity*.

The risks of fraud are considerable, but through sharing real life examples of fraud and attempted fraud, our hope is that your organization will be able to reduce and combat fraud.

The incidence of attempted fraud below is shared by a senior executive and treasurer in the real estate sector. Luckily, his story ended well, but it provides helpful information for all treasury and finance teams.

Fraud Prevention & Awareness

February 2015 when I was on vacation, I received a call from our company's assistant treasurer. He launched into a story about an interesting morning he had in my absence. The assistant treasurer described an email from our CEO, seeking to wire $8 million to execute an acquisition of a UK target company. Given the confidential nature of the transaction, the CEO asked that the assistant treasurer not discuss the wire with anyone else. For a number of reasons, I became concerned as I waited for my colleague to finish his story.

Having served for the last nine years as treasurer of our company, a leading real estate developer, owner and investor, my department and I had worked diligently to establish effective payment processes that would reduce the risk of fraudulent or inaccurate payments. These efforts can be split into four primary categories: Internal Controls, Information Technology & Dissemination, Corporate Culture and Monitoring/Compliance.

Internal Controls

We have established specific guidelines and procedures that must be followed in the preparation, approval and execution of electronic payments. These policies require the following:

- **Segregation of duties** – Each payment must have at least three separate employees involved before it will be processed. One employee requests the payment, one employee must process the payment and a final employee approves/releases the payment.
- **Physical and electronic forms** – We have a physical form to be filled out requesting a payment that includes the vendor's account information, a copy of an invoice and an original signature from an employee with sufficient authorization to approve the payment.
- **Payment authorization limits** – A delegation of authority is in place giving each employee a specific limit on the payment amount they can approve.
- **Bank controls** – We have ensured that each of our bank accounts has the proper controls including, but not limited to, positive pay and ACH debit block.

Information Technology & Dissemination

Our company use of information technology is critical to not only implement the internal controls described above, but also to rapidly disseminate information in order to ensure transactions are widely communicated to accounting and other key departments. Our company has had a treasury workstation for over twenty years, and the workstation allows us to define the requirements that need to be met for payments to be input and released. We currently use Kyriba as our treasury workstation and find it valuable in helping implement our internal controls. The Kyriba system is also set up to distribute key reports, including a list of payments being processed, several times a day. Finally, our Kyriba workstation has security administrators from our IT department that govern over user rights, ensuring that employees have access and authority that is consistent with their job requirements.

CASE STUDY

Corporate Culture & Employee Education

Our company seeks employees with high integrity and outstanding character, and this is especially important in the treasury department given the influence the team has over payment processing. The company's senior management understands the importance of payment policies and actively supports the treasury department's enforcement of payment protocols. The company also ensures the treasury department has the resources it requires to effectively execute its responsibilities. In terms of employee education, with the help of our internal audit department, we created an electronic payment processing policy that was distributed throughout the organization. In conjunction with internal audit and the IT department, the company has held mandatory seminars on payment fraud and reviewing best practices for preventing fraud from occurring.

Monitoring and Compliance

Daily report dissemination allows the company's accounting group to perform timely accounting reconciliations. These reconciliations should highlight fraudulent or inaccurate payments and prevent them from occurring in the future. The processing of payments receives significant attention during our regular internal and external audits. The treasury department tries to work closely with the internal audit department throughout the year to ensure we are implementing best-in-class protocols to protect our company's interests.

Turning back to that day in February, the assistant treasurer informed me that they had not processed the $8 million payment. While the transaction appeared credible and the email effectively mimicked the writing style of our CEO, the email was in fact, a fraud attempt. As the assistant treasurer pondered what he thought was the CEO's request, he realized that for a number of reasons he would be unable to follow the CEO's instructions.

- First of all, a second employee would have to be involved to input the payment into the company's workstation and the CEO has asked for strict confidentiality.
- Also, the assistant treasurer does not have the authority to release a wire as high as $8 million.
- Finally, any payment request would require the company's payment authorization form be filled out, with only the CEO having the authority to personally sign off on the amount.

When the assistant treasurer walked down to the CEO's office to discuss these questions, it quickly became apparent to both of them that this email was fraudulent.

Fortunately, this story has a happy ending, but I am well aware that the end result could have been dramatically different if not for the guidelines and procedures we had put in place to prevent against payment fraud attempts such as this.

About Kyriba

Kyriba is the global leader in cloud-based Proactive Treasury Management. CFOs, treasurers and finance leaders rely on Kyriba to optimize their cash, manage their risk, and work their capital. Our award-winning, secure, and scalable SaaS treasury, bank connectivity, risk management and supply chain finance solutions enable some of the world's largest and most respected organizations to drive corporate growth, obtain critical financial insights, minimize fraud, and ensure compliance. To learn how to be more proactive in your treasury management and drive business value, contact treasury@kyriba.com or visit kyriba.com.

kyriba

*2016 AFP Payments Fraud and Control Survey – Report of Survey Results, March 2016. Underwritten by J.P. Morgan. Pages 6, 7 and 8 noted.