Payment Errors & Compliance Violations

KYRIBA FACT SHEET

Payment errors and compliance violations cause significant losses for businesses of all sizes. Fraud alone cost companies more than $42 billion last year, according to PwC's Global Economic Crime and Fraud Survey.

The repercussions are wide-ranging, from arduous public disclosures and legal fees to reputational damage. Some are the result of attacks by elite cybercriminals, while others are simple mistakes made by careless or inexperienced employees.

Kyriba's Payments Fraud Solution delivers confidence that payment fraud attempts, errors and policy violations are captured, identified, and eliminated, saving your organization time, effort, and money.

PAYMENT MANAGEMENT

Many treasury departments rely on ineffective solutions to process and execute their payments. When these systems fail to catch a violation, it can go undetected for weeks or months before someone notices and attempts to recuperate the funds. Today's challenges require preemptive solutions.

Kyriba Payments puts the control in the hands of the user while providing full support on the back end. Users can assign up to nine levels of payment approvals, which can all be made from the device of your choice. Multiple payment types are supported, and acknowledgements are always sent from the receiving bank.

Furthermore, Kyriba Payments gives treasury departments a fully automated, proactive system that recognizes potential problems before payments are executed. Using artificial intelligence and machine learning, Kyriba's module examines your transaction history and isolates anomalies. It can catch variances that humans can't, and constantly adapts when it uncovers problems.

kyriba

Kyriba detects and stops payments compliance violations before they happen by enabling standardized payment controls, ensuring that only authorized transactions are executed.

DETECTING AND HALTING PAYMENTS FRAUD

A failure in compliance often means success at payments fraud. According to the 2021 AFP Payments Fraud and Control Survey, business email compromise (BEC) scams surged last year as many companies moved to remote working models and verifying payment instructions became more challenging. Fully 61% of respondents view their accounts payable (AP) departments as being susceptible to BEC.

Kyriba Payments Fraud Detection supports the CFO's internal governance procedures and controls framework:

Irregular Payment Patterns

Fraudsters now use artificial intelligence (AI) in their efforts to penetrate corporate defenses. CIOs can up their game by also incorporating machine learning (ML) algorithms into their payment audits. The ML program screens every new payment against the payment history, identifying – and quarantining – suspicious payments for further review. While in prior decades this analysis would have been done manually, the speed and data requirements to fulfill this task today make automation a necessity.

Bank Account Validation

Using application programming interfaces (APIs), Kyriba connects, in real-time, to cloud-managed databases and confirms that the bank accounts being credited to in the payment instructions belong to the intended counterparty. This is one important layer of protection in the fight against BEC scams and other phishing attempts. Until the advent of API connectors, this validation was never a part of the ERP-to-bank payment journey.

Payment Policy Screening

Every CFO has a comprehensive payment policy, documenting the review, approval, and denial procedures for their organization's payment scenarios. These policies have multiplied in complexity, as new examples are introduced, often in response to fraud exposures and attempts. The challenge for CFOs is screening every single payment that goes out the door against these payment policies. While CIOs can digitize payment policies, the algorithms and data required to identify and quarantine suspicious payments require more advanced automation that API-driven connectivity platforms are ready to support.

kyriba

ELIMINATING DUPLICATE PAYMENTS

Among the most significant and frequent types of violations that occur are duplicate invoice payments. Duplicate payments can result in time-consuming investigations, significant efforts to recuperate money, compliance consequences, and reputational damage.

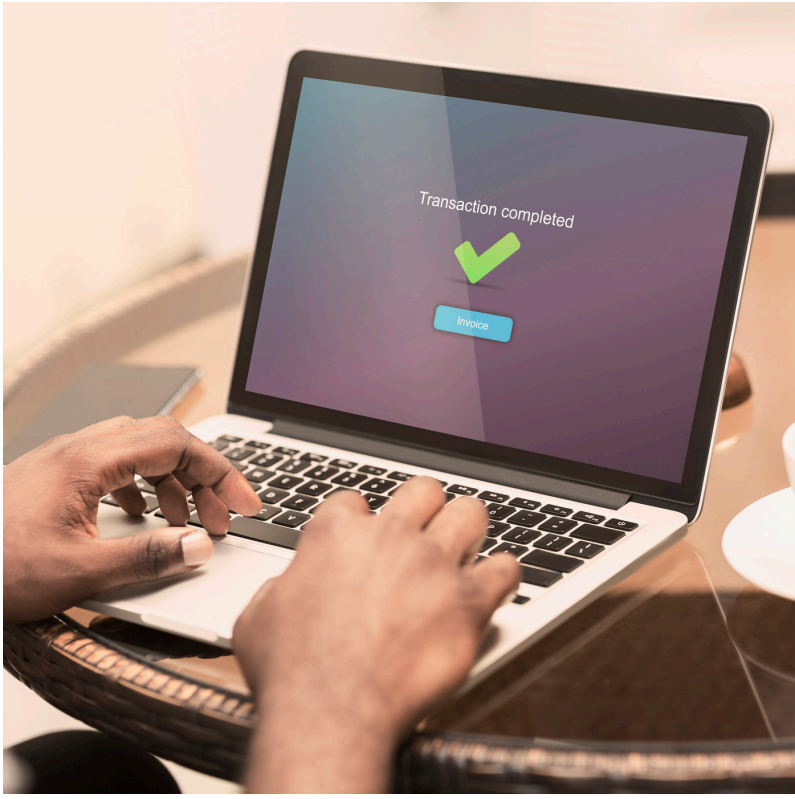
While duplicate payments can stem from fraud, they also come about without any malicious intent. Oftentimes, a merger or acquisition will see two AP teams and/or ERP systems not working in tandem. This can lead to invoice payments being made multiple times, even though ERP systems are typically set up to prevent these types of errors. Duplicates can also result from errors in vendor master data, or payment terms being applied incorrectly.

Large amounts of duplicate low-value/high-volume payments, which often go unnoticed for large periods of time, can result in substantial losses and lengthy investigations. Meanwhile, a small amount of duplicate high-value/low-volume payments might be noticed quickly but will surely have immediate repercussions on an organization's cash flow. Kyriba's Fraud Module has exceptional screening capabilities to detect and stop these errors before they happen.

Even stopping just one errant payment can prove to be imperative; last year, Kyriba halted a payment for a client that would have resulted in a $1.68 million loss. In 2020 alone, Kyriba saved its clients more than $350 million by stopping hundreds of duplicate payments.

THE CHOICE IS YOURS

Payments errors and compliance violations will continue to be an issue for any treasury department relying on ineffective management or antiquated systems. Modern threats call for modern solutions. Kyriba Payments is the only choice for challenges of today—and tomorrow.



kyriba