Ebook

Payments Fraud Detection in an Escalating Threat Environment

Kyriba

Contents

Introduction

Modern fraud threats are innovative and constantly evolving. To confront these threats, organizations that want to survive need to deploy the most up-to-date payments fraud detection and prevention solutions.

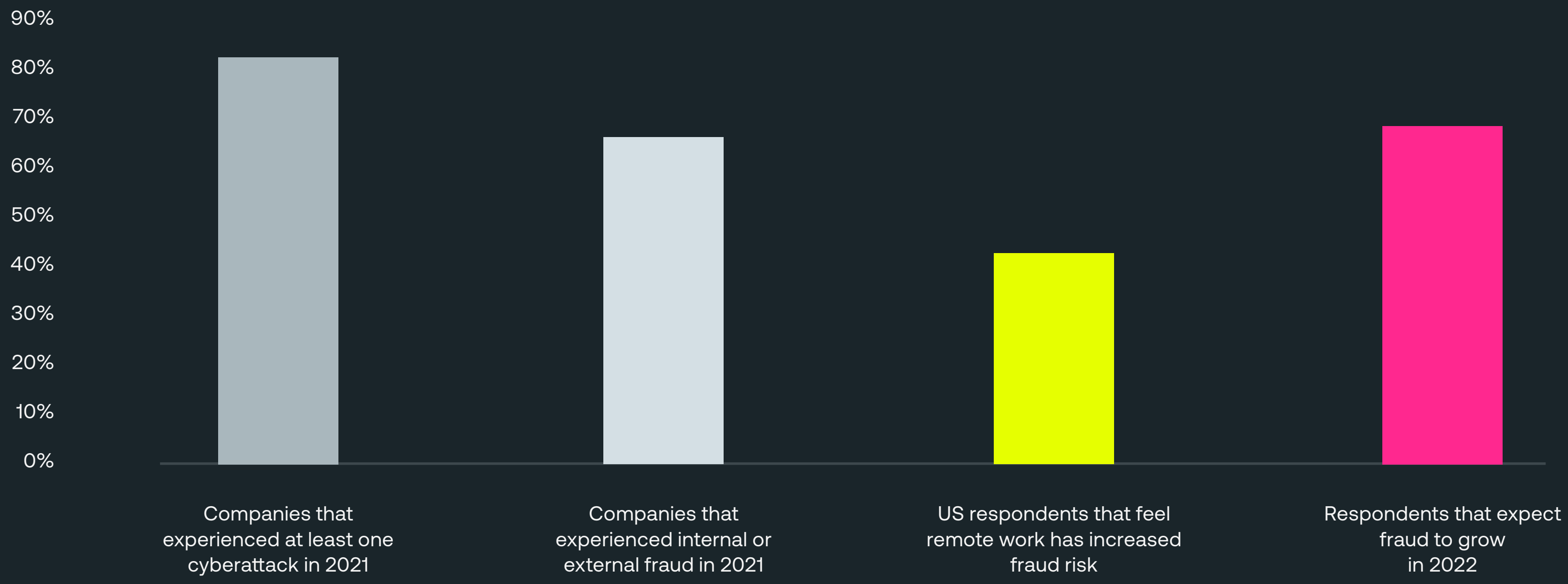
In this eBook, we will explore the most common fraud threats to businesses today and detail the leading, AI-based tools that CFOs and CIOs can use to stop attacks before they happen. We'll explore the ways that Kyriba solutions protect our customers, and impart that knowledge to you.

We'll also look into tools like artificial intelligence and machine learning (AI/ML) and application programming interfaces (APIs) are game changers in the fight against fraud. We understand and use these technologies, and it's time that you did as well.

The Changing Face of Fraud

Fraud threats have grown exponentially throughout the COVID-19 pandemic as the remote working environment has left companies struggling to ensure that employees are following strict security protocols. According to a 2022 KPMG survey of over 600 executives, the **shift to remote work has increased the risk of fraud**, and most companies experienced fraud incidents last year.

Fraud Outlook



Source: 2022 KPMG Fraud Outlook

The losses that stem from fraud are significant. Respondents reported an average profit loss of 1% from fraud and compliance violations in 2021. And the larger the company, the more criminals will target it.

Fraud Losses

42%

Percentage of companies that have experienced profit losses of 0.5% to 1% due to fraud

85%

Percentage of large companies that have experienced fraud losses in 2021

35%

Percentage of companies that have a program in place to prevent fraud

Need for Corporate Investment and Attention

With the pandemic continuing for the foreseeable future and challenging organizations' ability to operate and staff effectively to counter the ever-increasing fraud threat, it is surprising that over half of the companies surveyed say there will be no changes in their budgets to invest in anti-fraud measures.

With less than half of organizations today having a program in place to prevent, detect and respond to fraud, it is evident more focus on greater investments in their protections is called for. CFOs, treasurers and CIOs clearly require a more complete set of defenses in the form of new, leading, automated AI-based fraud detection.

Pervasive and Emerging Fraud Threats

Business email compromise (BEC) scams continue to plague treasury and finance departments. BEC scams typically begin with an urgent email sent to an employee that appears to come from a senior level official, requesting a money transfer. In actuality, a fraudster has copied a legitimate email address, usually after infiltrating a company's email system via phishing.

A variation of this scam consists of emailed invoices that appear to come from a routine supplier that have new instructions on where to send payment. According to the FBI's Cyber Division, there was a 5% increase in BEC adjusted losses from 2019 to 2020, with over $1.7 billion losses reported in 2019 and over $1.8 billion losses reported in 2020.

Check and wire fraud remains a significant problem for treasury and finance departments, as these are the payment methods most susceptible to fraud. AFP research found that 66% and 39% of financial professionals reported fraud activity via these two payment types in 2020. However, check fraud has been in decline in recent years as fewer organizations are using checks for B2B payments.

Deepfake voice fraud is a relatively new method of attack but one that has proven highly effective. This brand of fraud consists of criminals making calls using deepfake voice technology, software that can successfully copy a person's voice via a small audio sample.

Common Vulnerabilities For Organizations

Technical

- Lack of encryption on a platform
- Disparate systems and connectivity points (multiple ERPs with different workflows within them)

Processes

- Lack of standardization
- No systematic workflows to manage anything related to payment activity
- Lack of visibility to the audit trail

Human

- Compliance failure
- Inadequate training
- Errors in judgment
- Internal collusion

Deepfake voice fraud caught international attention last year when it was revealed that fraudsters used it to complete a $35 million bank heist.

Ransomware attacks, though not technically fraud, are nevertheless prominent threats to companies' systems and bank accounts and have surged in recent years. In a ransomware attack, a company's internal system is compromised (usually through phishing) and taken over. Users are instructed to either pay a ransom or permanently lose access to their systems.

Ransomware as a service (RaaS) is the latest innovation of this threat; it consists of developers selling or leasing ransomware exploits to customers who then unleash them upon unfortunate victims.

Tools to Protect Against Fraud

To combat the threats of today, your payments fraud prevention and detection solutions should include these capabilities:

- Automated payment processes to standardize controls
- Real-time screening of all payments data to identify suspicious transactions
- User-defined payments screening rules
- Resolution workflow to investigate suspicious payments
- An option to avoid alerting payments users who violated a payments rule
- Monitoring of the status and priority of alerts in a KPI dashboard

Modern payments fraud detection software like Kyriba's Payments Fraud Detection module offer these solutions and more.

Real-Time Screening, Alerts and Notifications

The rise of same-day and real-time payment systems has increased the need for real-time responses to fraud attempts. Modern fraud detection software uses artificial intelligence (AI) and machine learning to screen payments against historical payment data, pinpointing any anomalies. By providing more complete data, these solutions enable data-driven decision-making.

For example, Kyriba's Payment Fraud Detection solution determines the normality of each payment—whether automated or manual—flagging any with a low normality rank. The solution provides insights into the variables that determine payment normality, allowing users to see why one or more was deemed anomalous. And perhaps most advantageous for the user is that processes aren't slowed down in any way, even with greater visibility into payment data.

Payments could be flagged as anomalous for a variety of reasons, including:

- A high number of payments for the same third party
- Payments with unusually high amounts
- Payments to blacklisted countries according to company policy
- Suspicious changes to payments imported from an ERP
- Payments to a bank account used by several third parties
- Duplicate payments

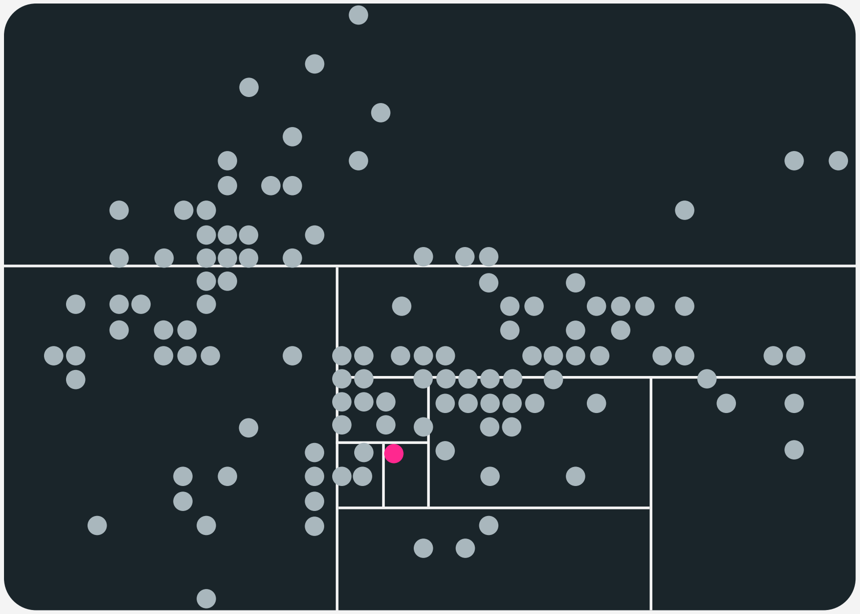
After testing multiple machine learning models, Kyriba's data scientists selected two solutions to identify irregularities in payments.

Isolation Forest

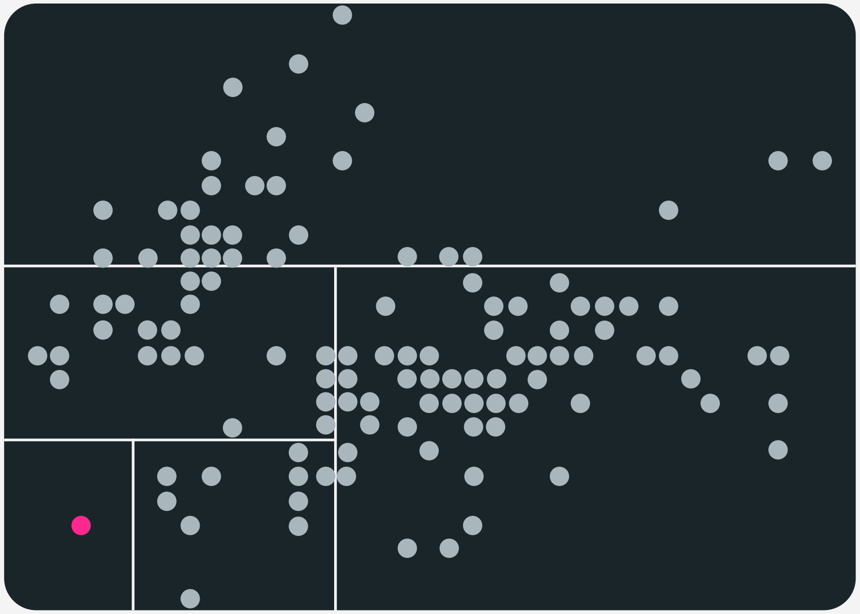
An isolation forest model is an unsupervised algorithm that works on the principle of isolation anomalies; anomalous instances in a dataset tend to be easier to separate from the rest of the sample.

In the following example, we can see that anomalies require fewer random partitions to be isolated, compared to normal points:

Normal Point: 8 Random Partitions



Anomaly: 4 Random Partitions



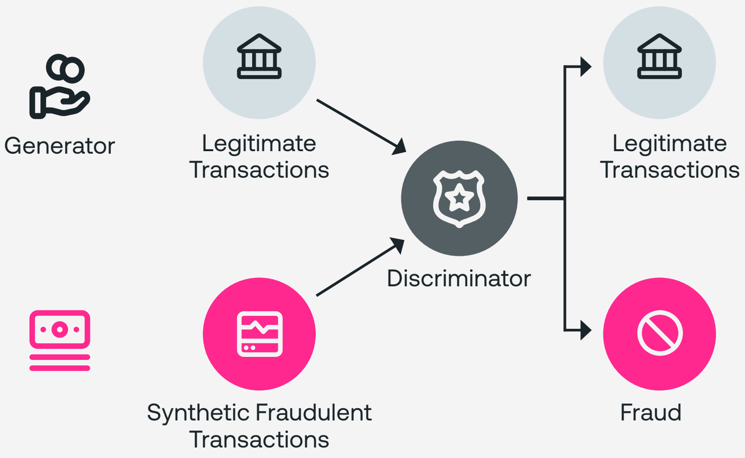
Generative Adversarial Network

One problem many machine learning models run into when trying to identify fraud is the lack of data around fraud. Most organizations haven't experienced significant payments fraud and thus lack the depth of examples to share. Others who may have been the victims of fraud may be reluctant or unable to share the specifics. So, training AI models can be challenging because the algorithms can only learn from good payments and, at best, a handful of bad ones.

Generative adversarial networks (GANs) can solve this problem. A GAN is a deep learning model that pits two separate neural networks against each other. One network (the generator) mixes real data and synthetic data together and attempts to outwit the opposing network (the discriminator).

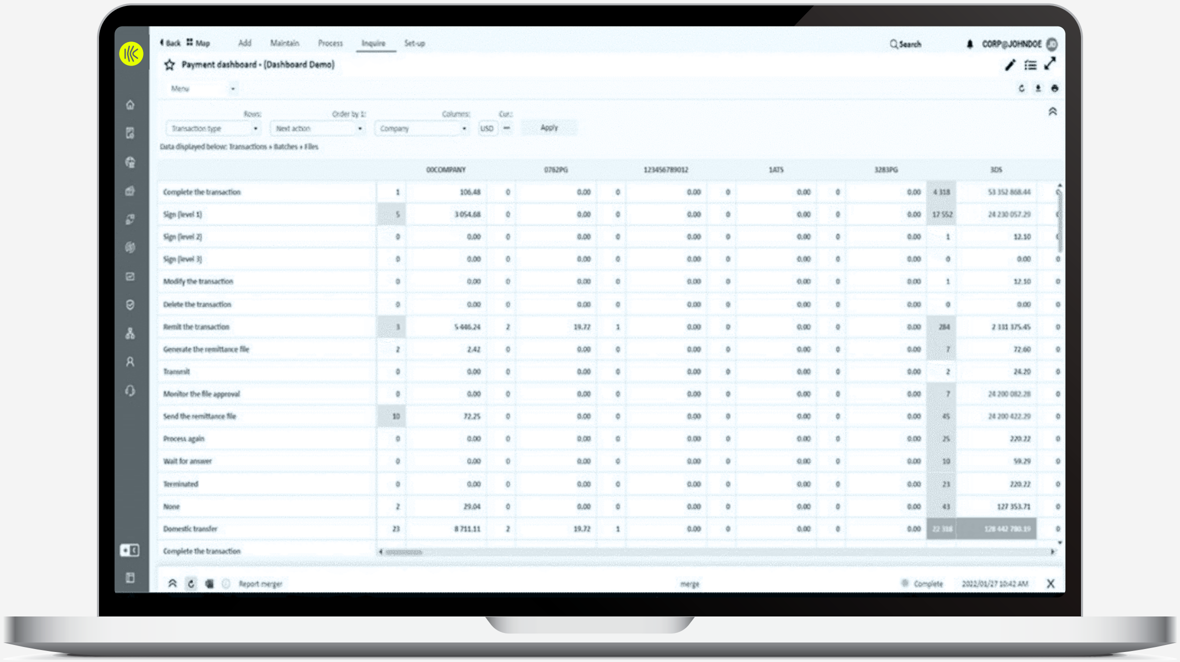
Kyriba creates a "fraudster" network (the generator), hiding synthetic fraudulent among legitimate transactions based on a client's payment history. Then, a "police" network (the discriminator) sifts through the data, separating the illicit transactions from the good ones. By training the fraud detection model on these competing networks, Kyriba can better identify fraudulent transactions when viewing real data.

Generative Adversarial Network (GAN) Model



Dashboards

Dashboards can be set up to display all suspicious payments and prioritize their resolution, based on factors such as detection rules, risk exposure, incident counts and a fraud detection scorecard. Dashboards provide authorized users with complete transparency into all payment screening and can resolve outstanding actions efficiently.



Payment dashboard - (Dashboard Demo)

Rows: Transaction type

Order by 1: Next action

Columns: Company

Cur.: USD

Data displayed below: Transactions + Batches + Files

	00COMPANY		0762PG		123456789012		1ATS		3283PG		3DS		
Complete the transaction	1	106.48	0	0.00	0	0.00	0	0.00	0	0.00	4 318	53 352 868.44	0
Sign (level 1)	5	3 054.68	0	0.00	0	0.00	0	0.00	0	0.00	17 552	24 230 057.29	0
Sign (level 2)	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	1	12.10	0
Sign (level 3)	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0
Modify the transaction	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	1	12.10	0
Delete the transaction	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	0
Remit the transaction	3	5 446.24	2	19.72	1	0.00	0	0.00	0	0.00	284	2 111 375.45	0
Generate the remittance file	2	2.42	0	0.00	0	0.00	0	0.00	0	0.00	7	72.60	0
Transmit	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	2	24.20	0
Monitor the file approval	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	7	24 200 082.28	0
Send the remittance file	10	72.25	0	0.00	0	0.00	0	0.00	0	0.00	45	24 200 422.29	0
Process again	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	25	220.22	0
Wait for answer	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	10	59.29	0
Terminated	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00	23	220.22	0
None	2	29.04	0	0.00	0	0.00	0	0.00	0	0.00	43	127 353.71	0
Domestic transfer	23	8 711.11	2	19.72	1	0.00	0	0.00	0	0.00	22 318	128 442 780.19	0
Complete the transaction													

Report merger

merge

Complete

2022/01/27 10:42 AM

Payments Fraud Prevention Workflows

Modern payments fraud detection modules also support fully automated, end-to-end workflows for the resolution of outstanding suspicious payments. Users can also determine how each detected payment should be managed, enforcing the separation of duties between the initiator, approver and reviewer of a detected payment.

Reviewers can also be determined by payment rule and specific scenario (e.g., the treasury manager reviews payments less than $1 million, while payments over $1 million go to the treasurer), and non-treasury personnel can be assigned to review certain detected payments.

Reporting and Audit Trails

Leading technology solutions can ensure that detected suspicious payments are permanently tracked in the system for daily, monthly or annual reporting. History is maintained indefinitely and all details of the suspicious transaction—including the audit trail of detected and resolved actions—are retained for internal and external audit reporting.

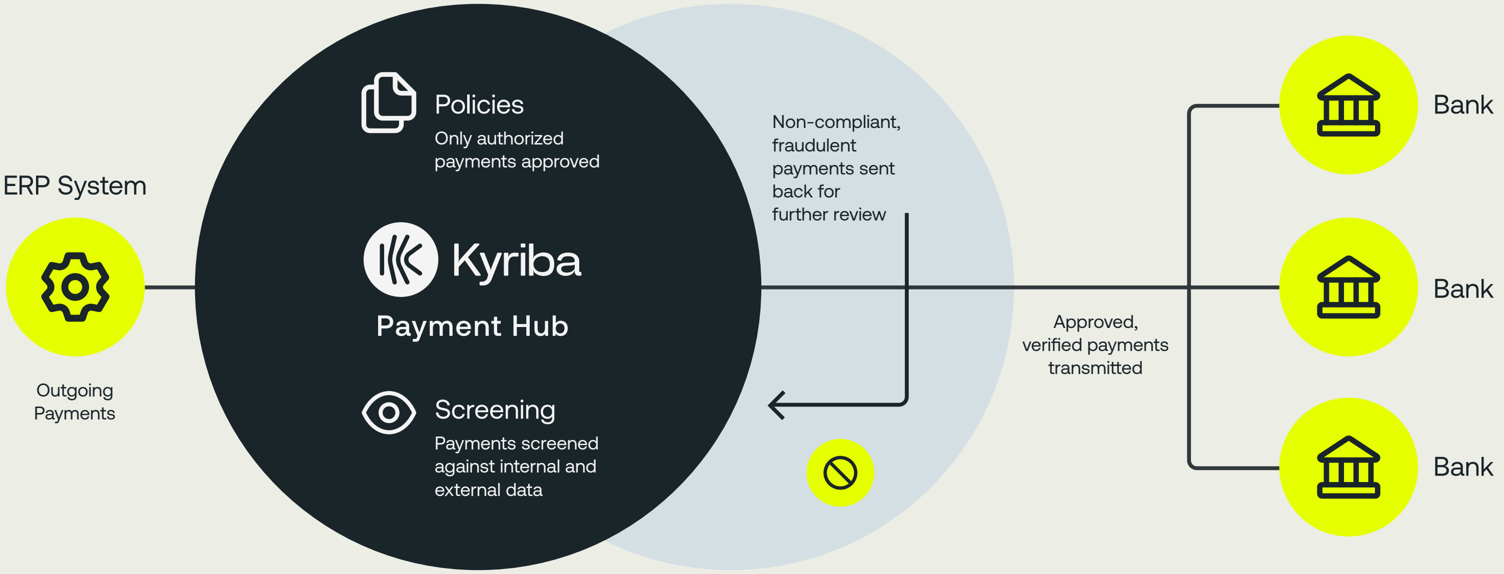
Payment Hubs

With a payment hub, organizations have all their fraud protection capabilities in one place. Payment hubs consolidate payment streams from ERPs, finance, treasury, legal, capital markets and decentralized teams, transforming disaggregated processes into a single source of record for all outgoing payments.

A payment hub also transforms payment data into bank-specific file formats and connects directly with global banks via multiple protocols, including host-to-host, SWIFT and regional networks.

Payments from ERPs or other systems can bring an entire enterprise-wide payments landscape under the consistent and risk-focused payments fraud detection framework. With API-driven connections and integration tied into an approval and payment fraud detection and prevention workflow, controls and fraud are enhanced and easily governed.

Payment Hub for Payments Fraud Detection


ERP System
Outgoing Payments
Policies
Only authorized payments approved
Kyriba
Payment Hub
Screening
Payments screened against internal and external data
Non-compliant, fraudulent payments sent back for further review
Approved, verified payments transmitted
Bank
Bank
Bank

Fraud Mitigation Matrix

Treasury and finance professionals have many payment fraud detection tools at their disposal. The following list of solutions provides an overview of some the capabilities that today's tools deliver for mitigating fraud risk.

Solution	Key Protections	Capabilities
Payment Fraud Detection Scenarios	Pre-Defined Detection Rules	• Flags unorthodox payments for further review • Easy to customize and come up with your own rules
Real-Time Screening	AI/Machine Learning Dashboard	• Screens payments against historical payment data • Displays all suspicious payments and prioritizes their resolution
Payments Fraud Prevention Workflow	Fully Automated Workflow	• Enables users to resolve outstanding suspicious payments • Allows users to determine how detected payments should be managed • Enforces separation of duties around a detected payment • Designates reviewer(s) by payment rule and specific scenario • Provides the ability to assign non-treasury personnel to review payments • Features an option to hide alerts from initiators/approvers of a payment • Allows scenario-based stopping of payments until resolved • Enable to bypass for low-value payments • Sets up tiered approvals
Reporting & Audit Trails	Complete KPI reporting	• Detected payments are permanently tracked in the system • History is maintained indefinitely

APIs: The Future of Payments Fraud Detection

Real-time payments, which are gradually becoming more prevalent, bring unprecedented visibility and transparency to both the payer and the payee. However, there is also no stopping the transfer of funds once a real-time transaction is executed. Therefore, fraud needs to be prevented in the approval process before a payment request reaches the bank.

Building APIs into the payment platform allows users to fully automate bank account validation and payment policy screening, identifying exceptions in real-time. APIs can instantly match payments against third-party data; for example, they can be used for sanctions list screening or verifying the ownership of the bank account to whom your company is paying.

By using APIs for third-party system integration with your payment platform, your organization can ensure real-time access to any needed database for account or compliance validation. Exceptional payments can be immediately quarantined for further review, while unexceptional payments process normally.

Learnings and Takeaways

- CFOs and treasurers require a more complete set of payments controls to mitigate modern fraud threats, including artificial intelligence/machine learning and APIs.
- Organizations have three common areas that make them vulnerable to fraud: technical systems, processes and human error.
- Modern threats include business email compromise scams, check fraud, wire fraud, deepfake voice fraud, and ransomware.
- Technologies that can be used to combat fraud include pre-defined fraud detection rules; real-time screening, alerts and notifications; payments fraud prevention workflows; reporting and audit trails; and payment hubs.
- As the threats continue to evolve, treasury and finance teams need to heighten their awareness.

Interested in learning how to build out payments fraud detection and incident response programs to maximize protection end-to-end? Check out this on-demand webinar. Cybersecurity and fraud experts from Corelight and Kyriba outline fraud defense strategies.

Select Brands Using Kyriba

爱回收
减 | 法 | 新 | 生 | 活
Baxter
Cenveo
GRAFF
HCSC Health Care Service Corporation
KOCH
ŞİŞECAM
Spotify
SOCIETE GENERALE
SPECIALIZED
TRANE TECHNOLOGIES

About Kyriba Corp.

Kyriba is a global leader in liquidity performance that empowers CFOs, Treasurers and IT leaders to connect, protect, forecast and optimize their liquidity. As a secure and scalable SaaS solution, Kyriba brings intelligence and financial automation that enables companies and banks of all sizes to improve their financial performance and increase operational efficiency. Kyriba's real-time data and AI-empowered tools empower its close to 3,000 customers worldwide to quantify exposures, project cash and liquidity, and take action to protect balance sheets, income statements and cash flows. Kyriba manages more than 35 billion bank transactions and $15 trillion in payments annually and gives customers complete visibility and actionability, so they can optimize and fully harness liquidity across the enterprise and outperform their business strategy. For more information, visit www.kyriba.com.