SAP Bank Connectivity: Increasing Payments Resilience in 2024

Steven Otwell
Director of Connectivity
Kyriba

Las Vegas

2024

SAPinsider

What We'll Cover

1) Understanding Your Risk
2) Protecting Your Payment Processes and Workflows
3) Best Practices to Secure Your Payment Journey
4) Q&A Discussion

Step 1 - Understanding Your Risk

Fraud Continues to be a Threat

- **46%** of organizations have experienced fraud, corruption or other types of economic crime

  Source: PwC's Global Economic Crime and Fraud Survey

- **92%** of finance leaders said payments fraud is as bad or worse than last year

  Source: AFP Payments Fraud and Control Survey

- **71%** of executives shared their organizations experienced internal or external fraud in the last 12 months

  Source: KPMG Fraud Outlook, 2022

- **62%** of treasury teams see the shift to faster and real-time payments as increasing risk of fraud

  Source: Strategic Treasurer Fraud & Controls Survey

- **96%** of US Companies were targeted with at least one fraud attempt in the past year

Source: Trustpair Fraud in the Cyber Era Report

Two New and Scary Technologies

(when fraudsters have them)

1) Deepfake

- Sounds (and looks) like your CFO or Treasurer
- Combined with “their phone number” and a good explanation = very difficult to catch in the moment

2) Large Language Models (LLM) *aka ChatGPT*

- Used for linguistically complex fraud schemes
- Eliminates ‘bad grammar’ phishing emails
- Emphasis on spear-phishing (targeted)

Most Common Corporate Payment Fraud Scams

Funds Transfer to Fraudster

- **Email from high executive asking you to wire funds to a "vendor" due to an emergency**

Third Party Scenario

- **Call from someone claiming to be business partner demanding payment**

Supplier Bank Account Change

- **Request to change supplier banking to fraudster's bank account**

Check Fraud & Direct Debit

- **Fraudulent check deposit or creation of a check**
- **Direct debit of company account**

Most Common Corporate Payment Fraud Scams

These schemes increase in complexity when fraudsters have access to your systems and data

Funds Transfer to Fraudster

- **Email from high executive asking you to wire funds to a "vendor" due to an emergency**

Third Party Scenario

- **Call from someone claiming to be business partner demanding payment**

Supplier Bank Account Change

- **Request to change supplier banking to fraudster's bank account**

Check Fraud & Direct Debit

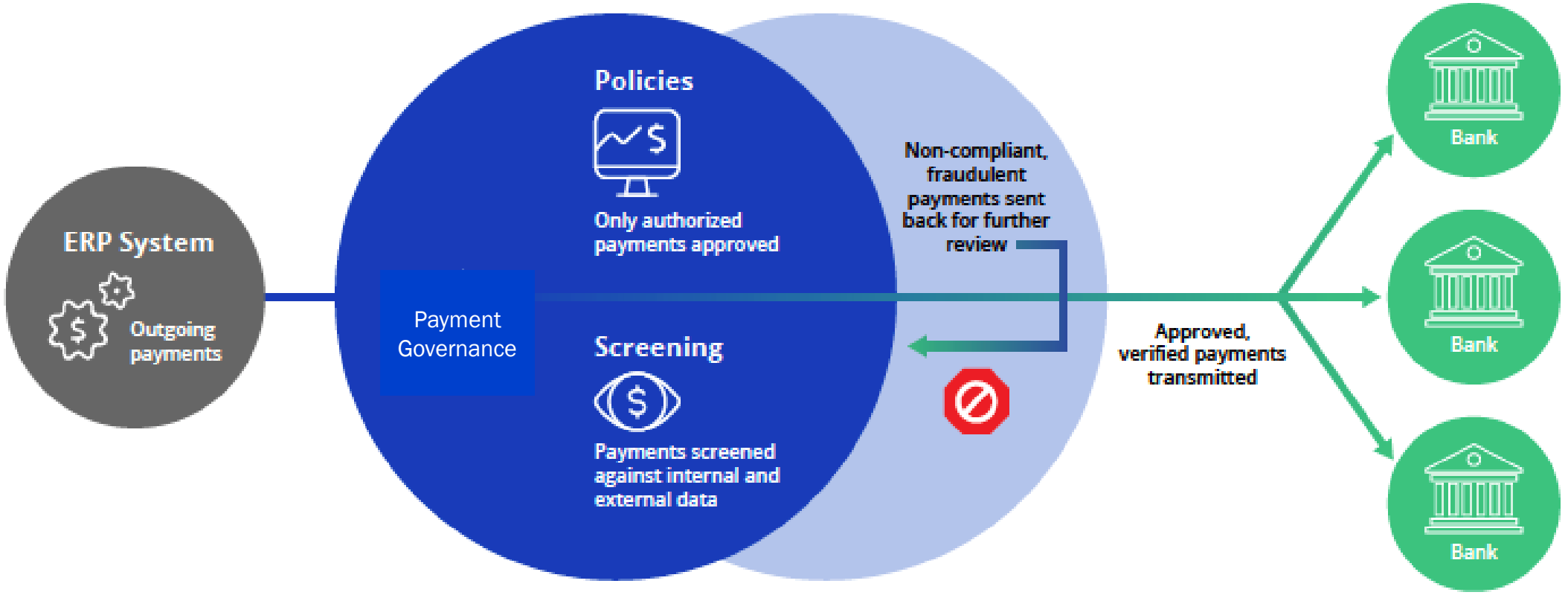
- **Fraudulent check deposit or creation of a check**
- **Direct debit of company account**

Corporates Must Protect Data and Process

- Even a good payment process is vulnerable if cybercriminals **have data**
  - Callback verification phone number actually connects to the fraudsters
  - CFO/Treasurers' calendars are compromised - so they know when your payment approvers are away
  - CFO/Treasurers' emails visible - to capture writing style
  - CFO's voice is publicly available (e.g. earnings calls)
  - Insider news (e.g. acquisition) is leaked or stolen

Step 2 – Protect Your Processes and Workflows

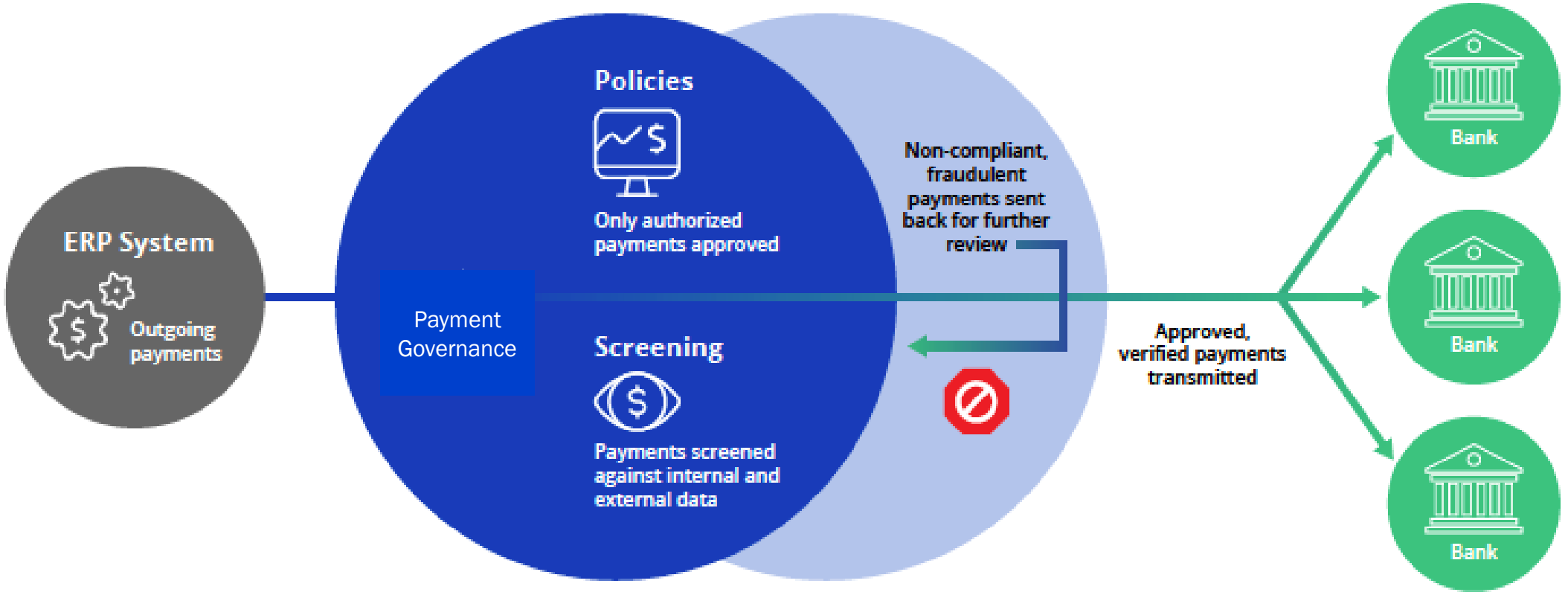
Resilience Against Fraudulent Payments



1) **Policies** - Digitize enterprise payment policies; approve only compliant payments
2) **Screening** - data-driven identification of suspicious payments -
   e.g. sanctions list screening, bank account verification, your payment history

Step 3 - Protect Your Processes and Workflows (with Data)

Injecting Data into your Payments Process



Two important technologies

1) **APIs** - connect systems, apps, and data in real-time
2) **AI** - leverage data to predict suspicious and non-compliant transactions

APIs: Connecting Payments Data in Real-Time

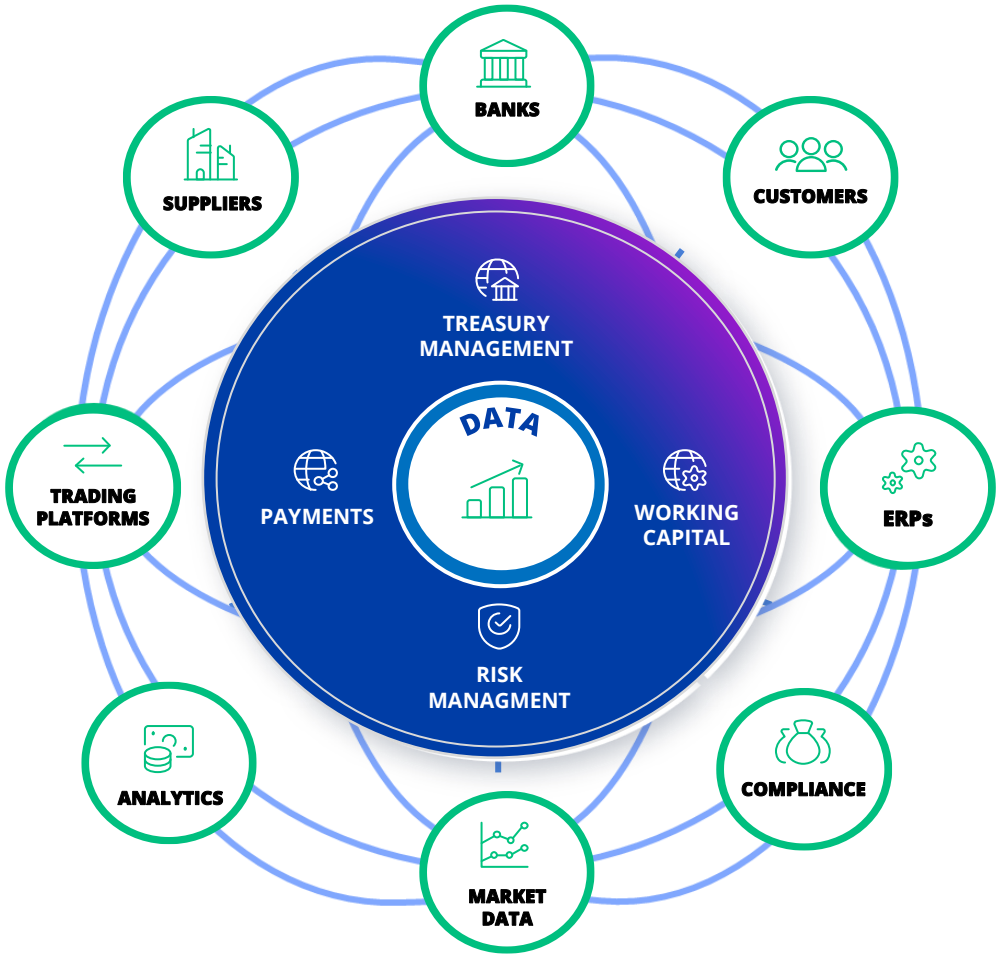
Enterprise Systems

SAP S/4HANA

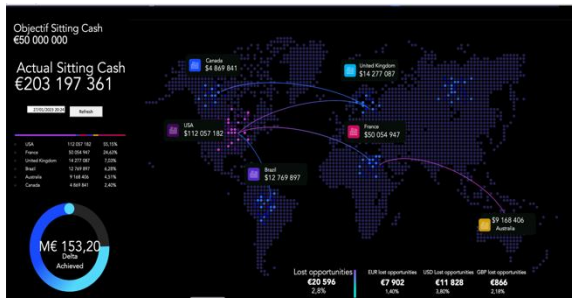
SAP ECC

Bank Connectivity

Citibank, J.P.Morgan, Wells Fargo, Fifth Third Bank, CaixaBank, Standard Chartered, HSBC, Bank of America, Societe Generale, BNP Paribas, Standard Bank, US Bank, ING, RBC, Santander, RBS



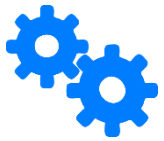
Reporting/Analysis



Embedded Apps

AI: Predicting Fraudulent Payments

There is a continuum of technologies ranging from performing computer keystrokes to mimicking human intelligence

Rules-based Automation	Machine Learning	Generative AI	Autonomous Intelligence
			
Rules Based	Pattern Based	Knowledge Based	Continuous Learning
Download and Reconcile Bank Statement	Identify Suspicious Payments Based on Historical Data	”Tell me when there is a fraudulent payment”	Design Our Payment Fraud Detection Strategy

Injecting Data into your Payments Process

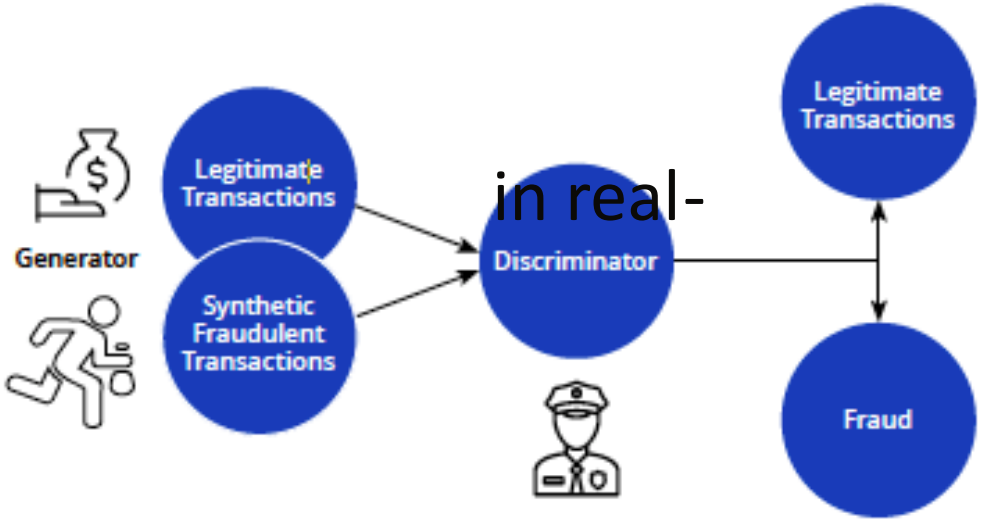
Artificial Intelligence

Train the model, so it learns from data

a) What is a legitimate payment?

b) What is not a legitimate payment (adversarial approach)?

c) Identify suspicious payments in real-time, at machine speed



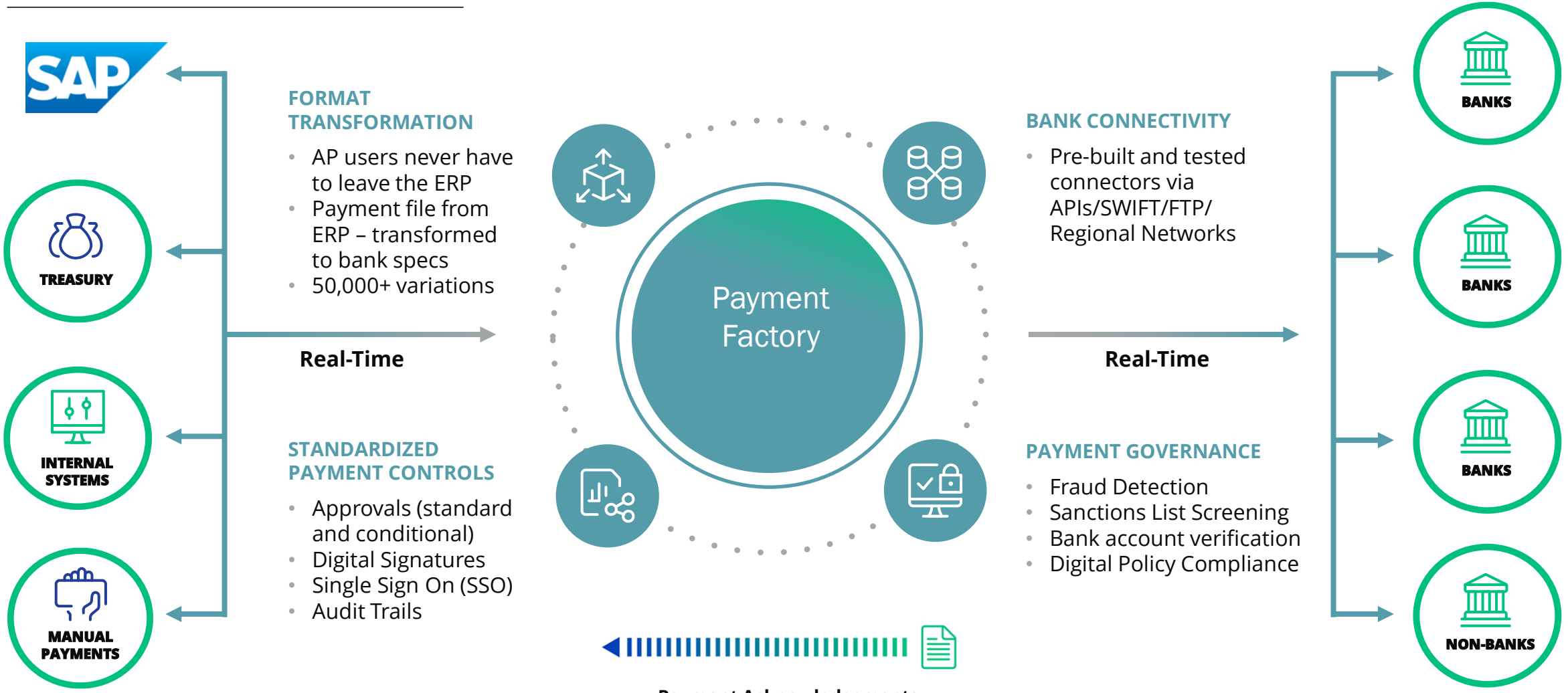
Real-Time is critical because:

a) **Instant Payments**

b) **Too much data for human decisioning**

Step 4 – Best Practices

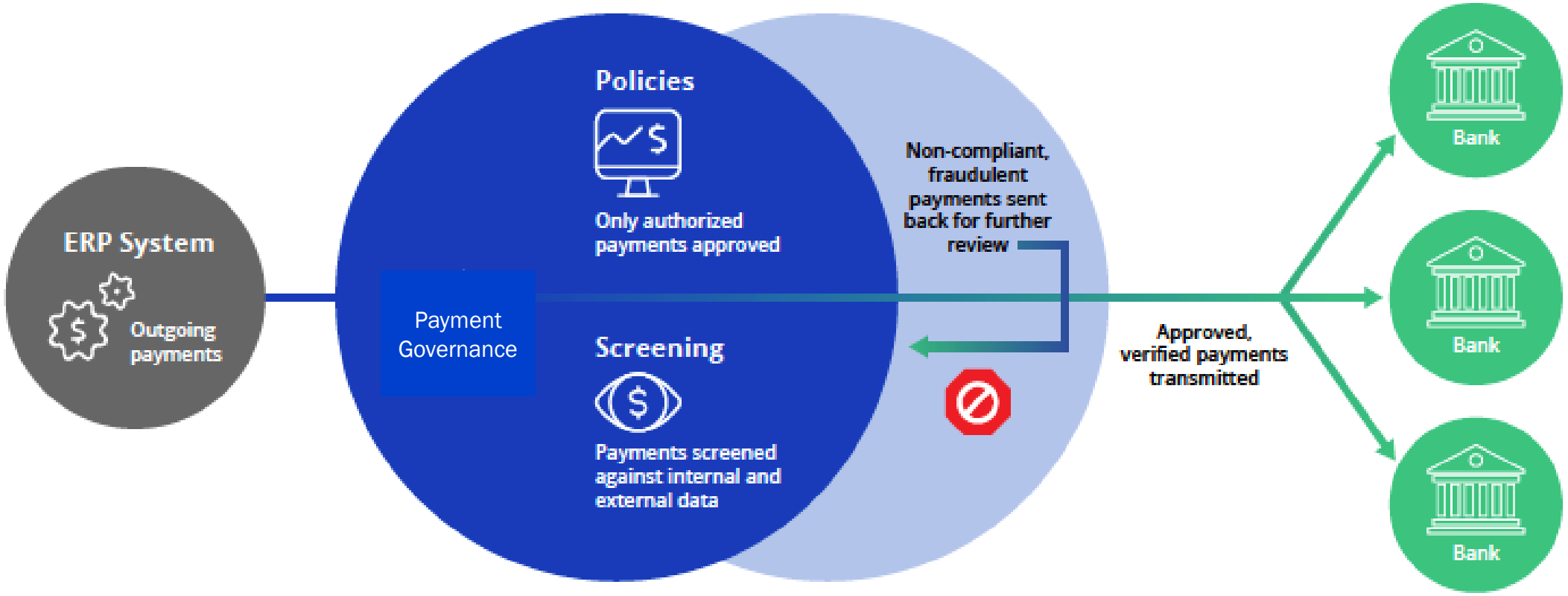
Today's Payment Journey



Considerations

- More sophisticated technologies being used in cyberwarfare and fraud incidents
- The need for real-time fraud detection to protect liquidity
- Building connective tissue between your fraud and threat hunting/IR programs
- Building the business case to invest in detection and response programs
- Opportunities for CFOs, CIOs and CISOs to heighten internal and external security

Injecting Data into your Payments Process



Entire Payment Journey is in real-time

- ✓ Initiation of payments from treasury or ERP platform
- ✓ Compliance and Governance screens out suspicious/non-compliant payments
- ✓ Verified instant payments settled in real-time

Wrap Up

Protection Against Payments Fraud and Cybercrime

- The most successful schemes attack your payments process after background data has been stolen
- Build connective tissue between your payments systems to improve defense at machine speed
- People design workflows; technology enforces process
  - ✓ Removes human bias and increases speed
  - ✓ Enables finance teams to move to real-time processing without adding risk

Data

Process

Human

Key Points to Take Home

1) Fraudsters have AI Technologies such as Deepfake and ChatGPT
2) Payment Fraud Schemes aren't as detectable as they used to be
3) Good Payments Governance Injects Data into Your Payments Process
4) APIs can deliver data and payment compliance checks in real-time
5) The adoption of faster and instant payments means that payment teams must move their processes to run at machine speed

Where to Find More Information

https://www.afponline.org/publications-data-tools/reports/survey-research-economic-data/Details/payments-fraud

- Annual survey and report by the Association for Financial Professionals benchmarking payment fraud data

https://www.kyriba.com/resource/cfo-guide-to-fraud-prevention-checklist/

- Resource to review payment fraud challenges and business practices

https://trustpair.com/white-paper/2024-fraud-trends-and-insights/

- Payment Fraud Report outlining the rising threat of payments fraud

Thank you! Any Questions?

Steven Otwell

Director of Connectivity

Kyriba

Please remember to complete your session evaluation.

SAPinsider

SAPinsider.org

PO Box 982Hampstead, NH 03841

SAPinsider comprises the largest and fastest growing SAP membership group with more than 800,000 members worldwide.