SAP Concur

Electronic Payment Fraud Management

Mark Merry, CPA, Assistant Director, Department of Financial Services, Division of Accounting and Auditing, State of Florida

Jim McClurkin - Director, Public Sector - SAP Concur

Nasser Chanda, CEO Paymerang

NASC 2020 Annual Conference | Branson, MO

SAP Concur

Agenda

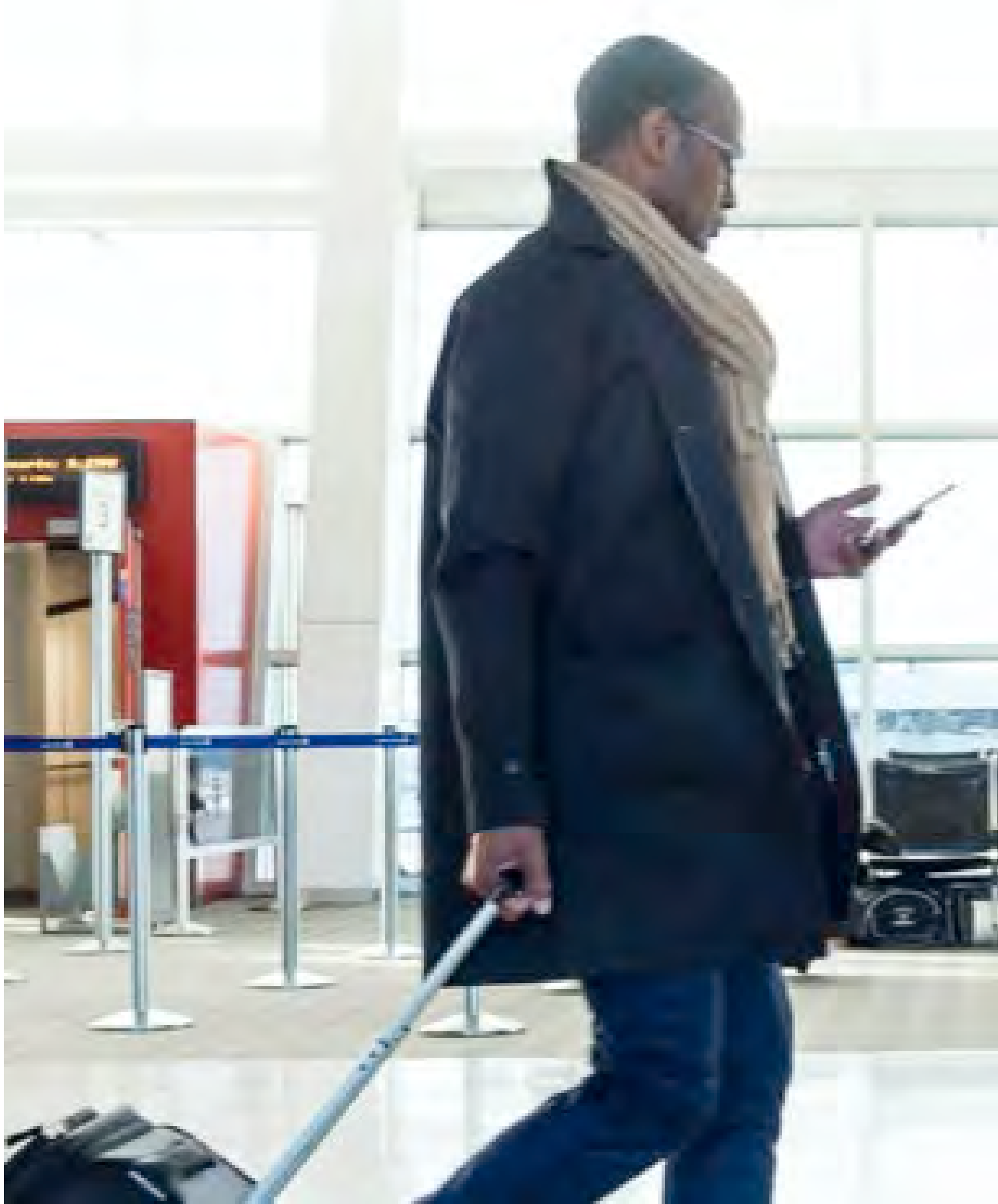
01 Introductions

02 SAP Concur

03 State of Florida

04 Paymerang

05 Questions



SAP Concur

Advancing Spend Management to Combat Fraud

How digital transformation can improve compliance and reduce risk

Jim McClurkin
Director, Public Sector
SAP Concur

March, 2020

THE BEST RUN SAP

Analyzing Risk for Government Agencies

$118k

Median loss per case

16%

of Reported fraud is in government

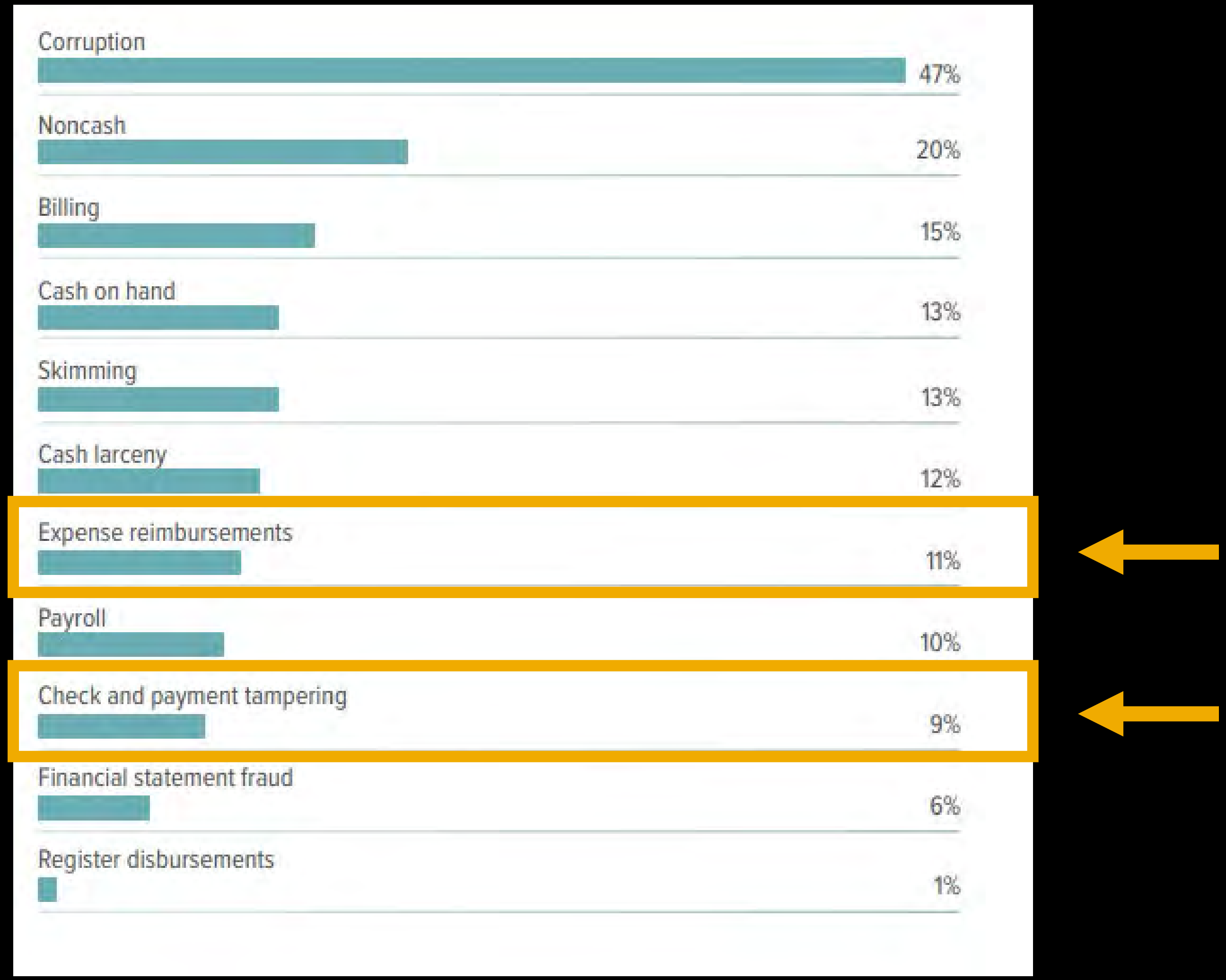
18 Months

Median time before detection

ACFE, Report to the Nations: 2018 Global study on occupational fraud and abuse | Government Edition

Most common fraud schemes in Government Agencies

20% of Fraud schemes within Government involve expense reimbursements and payments



Managing Spend in your Organization

Capture Challenges

- More spend and more transactions are occurring across more platforms
- Spend is becoming decentralized and is spread across more categories than ever before.

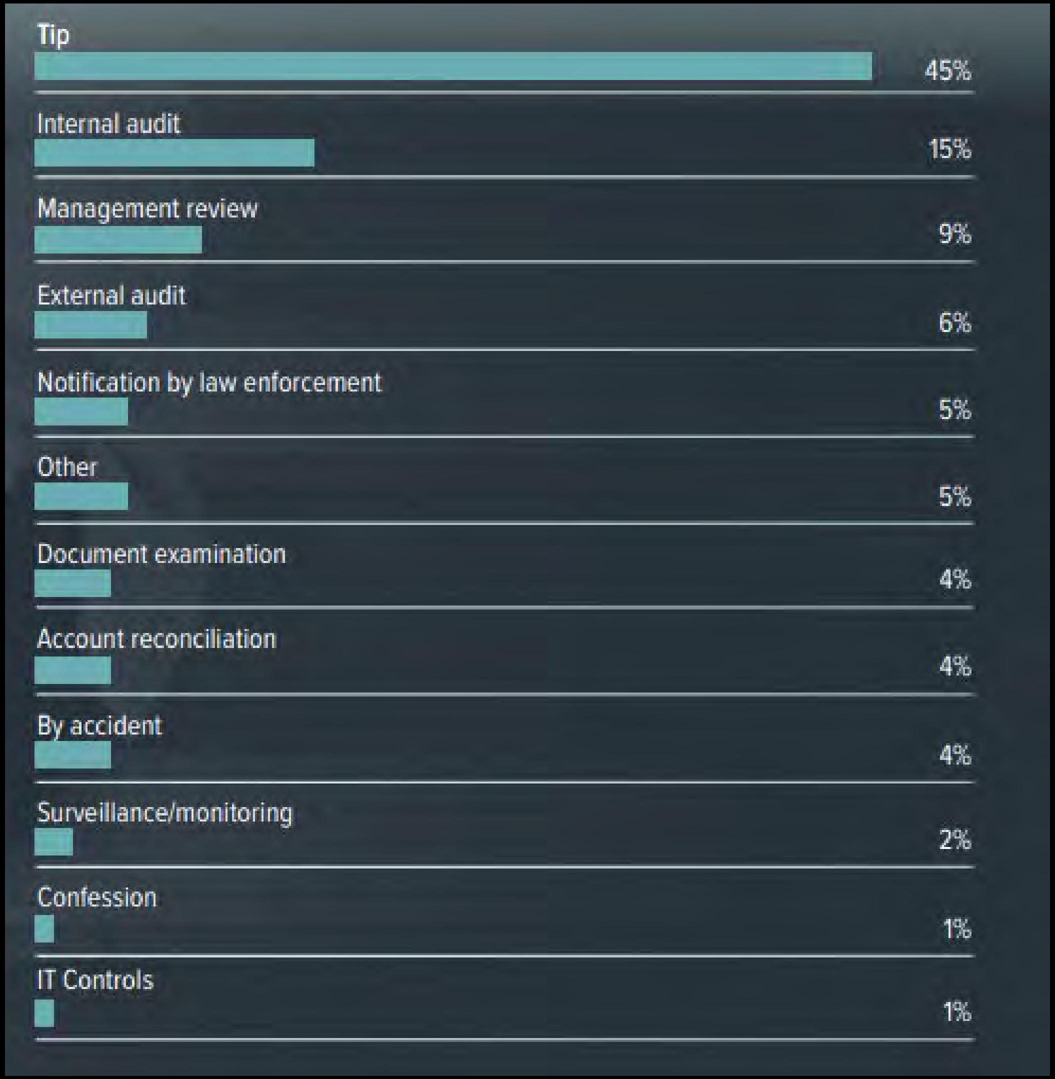
Financial and Compliance Challenges

- Lack of visibility and control of spending
- Slow financial processing, posting, and payments
- Changing regulations and policies

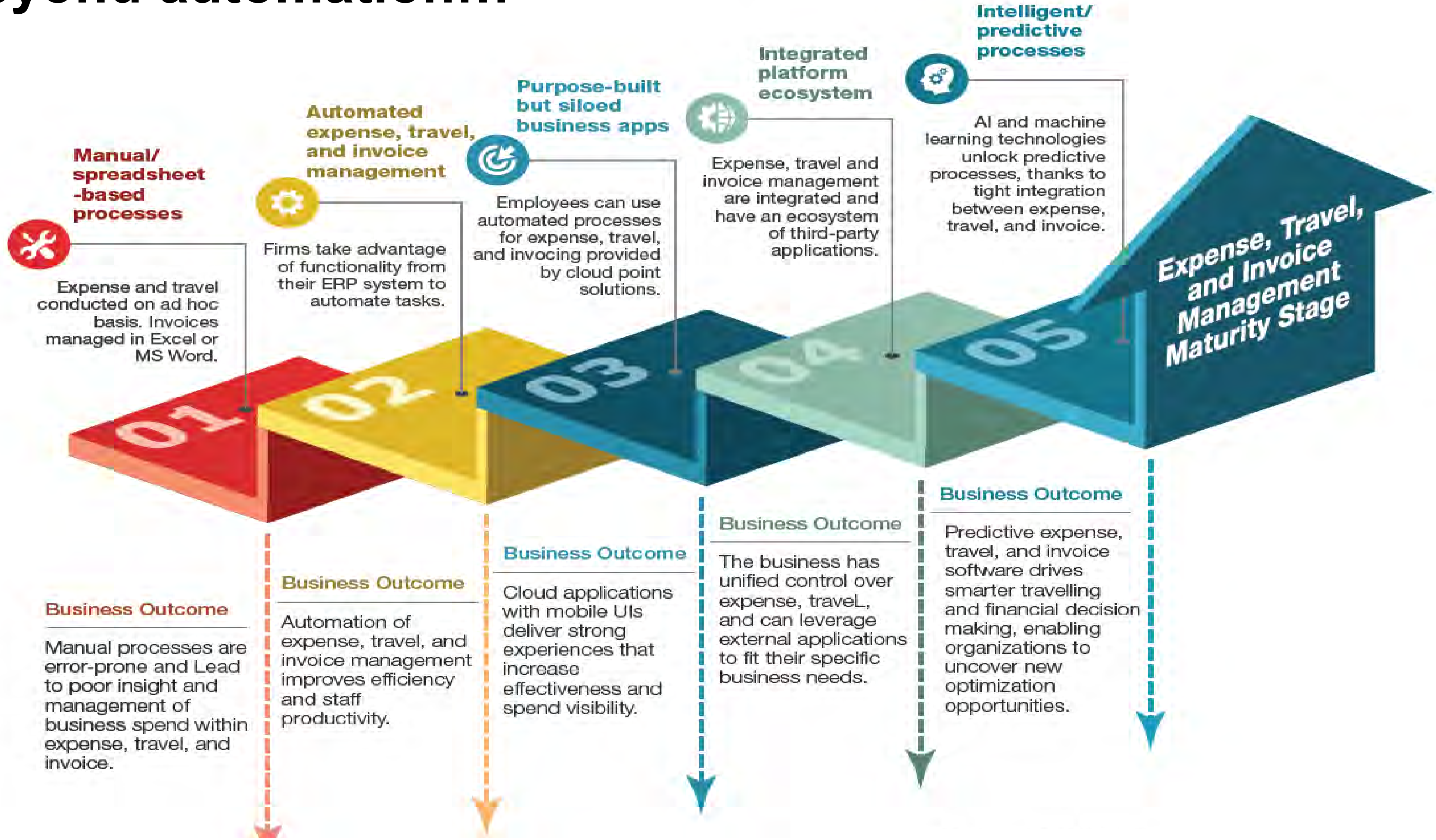
How is fraud initially detected?

45% of fraud detection relies on tips.

What if you could *automatically* audit 100% of expense and invoice requests before a payment is made?



Move beyond automation…



Manual/ spreadsheet -based processes

Expense and travel conducted on ad hoc basis. Invoices managed in Excel or MS Word.

Business Outcome

Manual processes are error-prone and Lead to poor insight and management of business spend within expense, travel, and invoice.

Automated expense, travel, and invoice management

Firms take advantage of functionality from their ERP system to automate tasks.

Business Outcome

Automation of expense, travel, and invoice management improves efficiency and staff productivity.

Purpose-built but siloed business apps

Employees can use automated processes for expense, travel, and invocing provided by cloud point solutions.

Business Outcome

Cloud applications with mobile UIs deliver strong experiences that increase effectiveness and spend visibility.

Integrated platform ecosystem

Expense, travel and invoice management are integrated and have an ecosystem of third-party applications.

Business Outcome

The business has unified control over expense, traveL, and can leverage external applications to fit their specific business needs.

Intelligent/ predictive processes

AI and machine learning technologies unlock predictive processes, thanks to tight integration between expense, travel, and invoice.

Business Outcome

Predictive expense, travel, and invoice software drives smarter travelling and financial decision making, enabling organizations to uncover new optimization opportunities.

IDC Travel and Expense Management Maturity Model, 2018

Provide More Control and Visibility
Before, During and After Spend Occurs

Leverage digital transformation and technologies such as Machine Learning and AI to prevent and detect fraudulent spend activities within your organization.

- **Using AI:** Discover where unauthorized and unnecessary spend is happening.

- **More Visibility:** Take control of spending processes, regulate policies, and save time, money and resources.

- **Reduce Risk and Increase Compliance**

- **Safeguards:** Prevent personal expenses from being paid out, stop processing of duplicate payments

Mark Merry, Assistant Director

Department of Financial Services

Division of Accounting and Auditing

State of Florida

An overview of the Department's EFT Process for Payments

Department of Financial Services
Division of Accounting & Auditing

Presented by: Mark Merry, CPA

Assistant Director

Our EFT process began in 1983-84

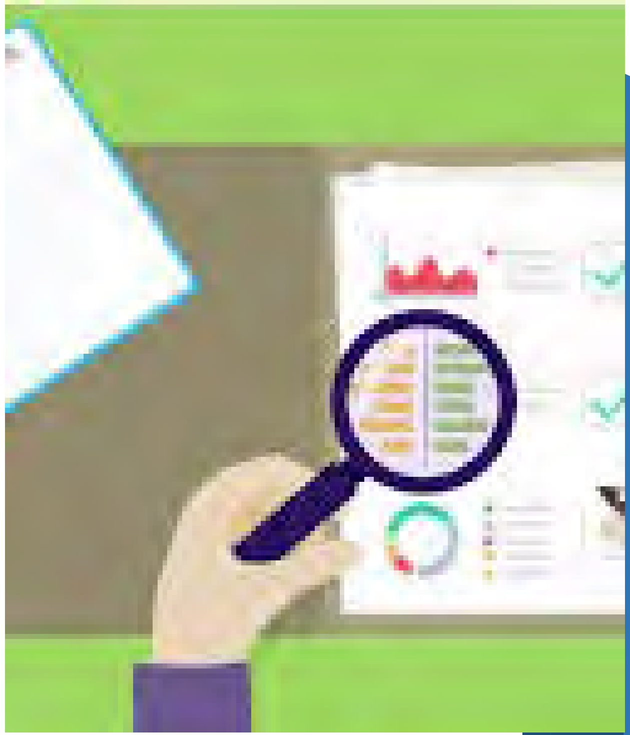
- ➢Payrolls were the first to be implemented
- ➢Retires were next
- ➢By 1990, we started bringing vendors on board
- ➢Very much a manual validation process with signed documents and corroborating information

After year 2000, employees and retirees were validated on the front end through the human resource and retirement systems

These systems provide user access controls where individuals can update their bank account information online

In 2008, Florida had a major EFT diversion in excess of $6 million

- The perpetrator used transparency website and contractor information to complete an EFT change request
- Using false information he was able to open a bank account
- Funds were diverted to this account and then transferred to a foreign country
- The fraud was detected quickly and $2 million was reversed before going overseas
- Through litigation, the bank paid $4 million to the State
- Individual was apprehended by the FBI at the Ft. Lauderdale International Airport



Today, the vendor EFT process continues to rely heavily on paper documents and manual validations which are time consuming and cumbersome

Where we want to go:

- Secure online portal where vendors can provide tax and bank account information in electronic format
- Many of the validations can occur online through our banking services contract, Lexus Nexus and through other State agency business systems
- Some manual validations would still be needed

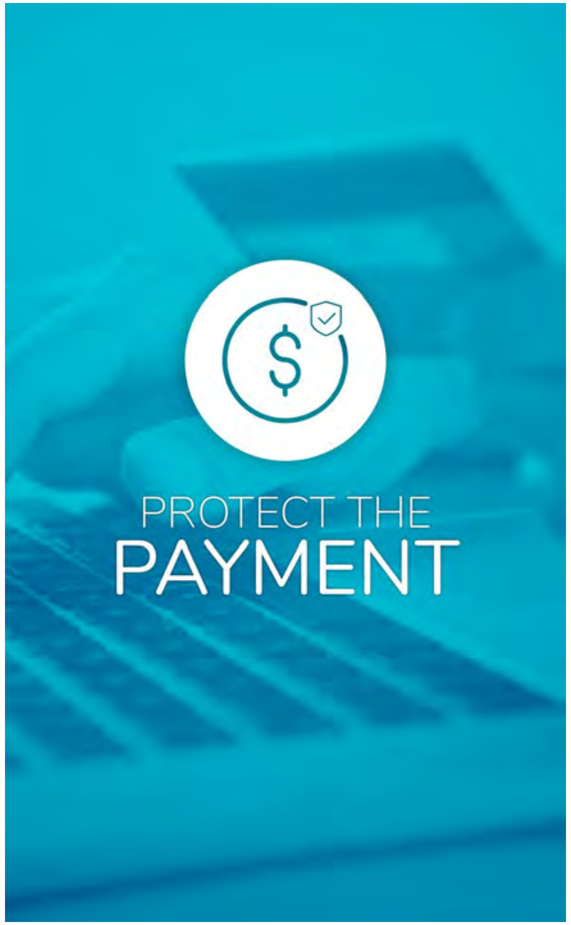
Nasser Chanda, CEO

Paymerang

paymerang SM

Are You Protected Against Payment Fraud?

FOUR LAYERS OF PROTECTION AVAILABLE



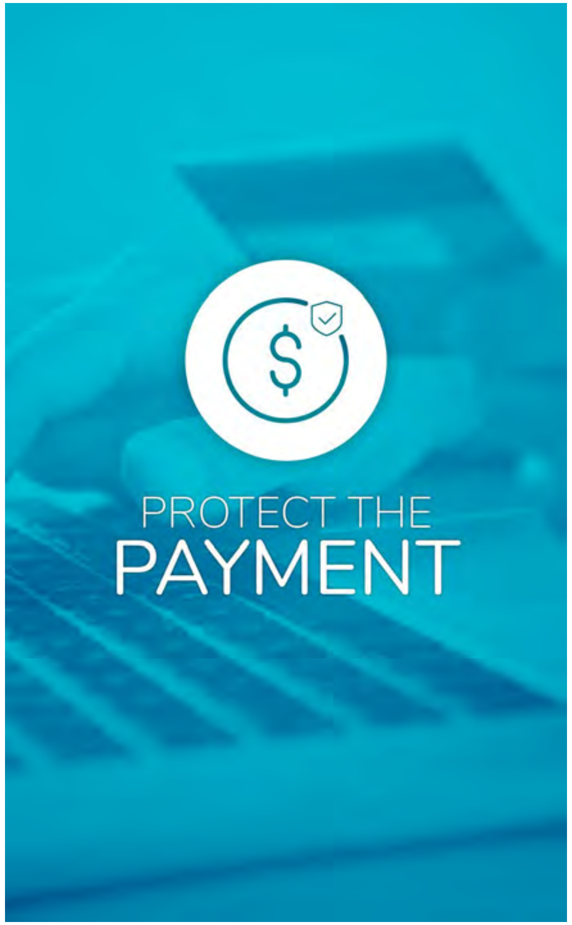
PROTECT THE
PAYMENT

SECURE THE
OPERATIONS

FORTIFY THE
NETWORK

LOCK DOWN
COMPLIANCE

PROTECT THE PAYMENT



POSITIVE PAY

WHY: To ensure only the authorized party on a check is allowed to cash that check and reduce the likelihood of payment to a fraudulent entity.

HOW: Enroll in the Positive Pay service at the financial institution where check payments are sourced.

VIRTUAL CARDS

WHY: To limit the exposure of open, higher limit credit lines that are in use for payments.

HOW: Transact using VISA virtual debit cards (vCards) to limit payments to a one-time use, preloaded payment amount.

ACH PAYMENT

WHY: Use of electronic payments that can be trusted through an established network, where the likelihood of fraud is reduced.

HOW: Register to use ACH payments with the bank account where payments are sourced and take additional steps to protect the payment information (i.e. encrypt sensitive data).

PROCEDURES

WHY: Procedures need to be in place to validate payment relationship information before action is taken to modify accounts or payments.

HOW: Before engaging with vendors or making any changes to information, the identity of the other party must be verified. Limit the information your employees can see and do not allow them to change sensitive data without approvals.

SECURE THE OPERATIONS

SECURE ENVIRONMENT

WHY: All payment data needs be protected in the operating environment where processed.

HOW: Use a combination of a clean desk policy, removal of all payment information from open office view, and a certified shredding service.

TRAINING

WHY: The payment team members are an important line of defense for ensuring a secure operation.

HOW: Conduct security awareness training by qualified staff on a regular basis to ensure team is aware of threats and how to detect suspicious links or fraudulent email addresses. Provide ongoing payment threat awareness information so the team knows what is considered suspicious and are ready to respond to it.

FRAUD DETECTION

WHY: To detect fraudulent payments and ensure that only legitimate payments are made.

HOW: Verify any anomalous changes made to vendor account information before processing payments. Assign fraud scores based on recent account changes.

PROCEDURES

WHY: To ensure operational controls are present throughout the payment process.

HOW: Set up all payment processes with multiple approvals, single payment limits and segregation of duties. Implement job rotation and cross-training for payment team members. Appropriate access controls.

FORTIFY THE NETWORK

END POINT PROTECTION

WHY: To ensure that only safe and trusted software run on computers that process payments.

HOW: Provide protection with the use of anti-virus software coupled with best in class application whitelisting technology to protect against forms of malware.

EMAIL DEFENSES

WHY: To reduce the amount of unsafe email into the payment process and protect sensitive information sent in payment email.

HOW: Deploy layers of spam/phishing defenses, including spear phishing detection, along with email encryption and rights management to protect sensitive email content.

VULNERABILITY MANAGEMENT

WHY: To identify exploitable software and security weaknesses in the payment system in order to reduce exposure to possible system compromise.

HOW: Enable a vulnerability management program with regular security posture scanning, software patching, and expert penetration testing.

THREAT PROTECTION

WHY: To determine when suspicious actions are being attempted or carried out against the payment system.

HOW: Enact intrusion and anomalous behavior detection capabilities with multi-factor authentication and full logging in the appropriate layers of the payment system.

LOCK DOWN COMPLIANCE

NACHA

WHY: To ensure automated payments are processed in a trusted and controlled environment.

HOW: Process payments using the ACH Network which maintains the highest level of safety and security for its participants through governance oversight by NACHA.

PCI

WHY: If payment cards are processed or stored there is a security standard mandated by the Payment Card Industry (PCI) that must be attested.

HOW: Implement the PCI Data Security Standard (PCI-DSS) to ensure that cardholder data is maintained in a secure environment accordingly.

SOC-2

WHY: To verify the operating effectiveness of a service provider's Availability, Integrity and Confidentiality (AIC) security controls, by an audit expert, for companies wanting to use the service.

HOW: If you are a service provider, then contract an audit service to conduct a SOC-2 assessment, in accordance with AICPA Trust Service Criteria.
If you are a consumer of a supplied service, then request the SOC-2 Report from the supplier and confirm any gaps in expected controls.

OFAC LIST

WHY: To reduce the likelihood of payments being sent to individuals or organizations determined to be threats to US national interests.

HOW: Compare the US Treasury Office of Foreign Assets Control (OFAC) Sanctions List against pending payments and stored supplier data to identify possible threats.

PRACTICAL STEPS

As long as there is money and valuable data, there will be fraud attempts and threats to security.

PAYMENT

- Positive pay
- E Pay
- Use one-time use, preloaded virtual cards
- Encrypt account information
- Verify vendors before making changes
- Limit employee access
- Require approval for changes

OPERATIONS

- Clean desk and secure documents
- Utilize certified shredding service
- Verify anomalous changes
- Assign fraud scores
- Suspicious links and fraudulent email detection training
- Multiple approvals
- Single payment limits
- Segregation of duties
- Job rotation and cross training
- Defined access controls

NETWORK

- Antivirus Software and whitelisting technology
- Vulnerability management program
- Security posture scanning
- Software patching
- Expert penetration testing
- Spam and phishing defenses
- Email encryption
- Multi-factor authentication

COMPLIANCE

- NACHA - read it, learn it, train it
- Do not store banking data if you can avoid it
- PCI- Secure cardholder data
- SOC 2- Security controls for integrity and confidentiality
- OFAC- Know your vendor and where your money is going

Q&A

Contact information:

Jim McClurkin
Director, Public Sector
SAP Concur
james.mcclurkin@sap.com

Mark Merry
Assistant Director, Division of Accounting and Auditing
State of Florida
mark.merry@myfloridacfo.com

Nasser Chanda
CEO
Paymerang
nchanda@paymerang.com

SAP Concur

Follow all of SAP Concur

Learn more at concur.com

The information contained herein may be changed without prior notice. Some software products marketed by SAP SE and its distributors contain proprietary software components of other software vendors. National product specifications may vary.

These materials are provided by SAP SE or an SAP affiliate company for informational purposes only, without representation or warranty of any kind, and SAP or its affiliated companies shall not be liable for errors or omissions with respect to the materials. The only warranties for SAP or SAP affiliate company products and services are those that are set forth in the express warranty statements accompanying such products and services, if any. Nothing herein should be construed as constituting an additional warranty.

In particular, SAP SE or its affiliated companies have no obligation to pursue any course of business outlined in this document or any related presentation, or to develop or release any functionality mentioned therein. This document, or any related presentation, and SAP SE's or its affiliated companies' strategy and possible future developments, products, and/or platforms, directions, and functionality are all subject to change and may be changed by SAP SE or its affiliated companies at any time for any reason without notice. The information in this document is not a commitment, promise, or legal obligation to deliver any material, code, or functionality. All forward-looking statements are subject to various risks and uncertainties that could cause actual results to differ materially from expectations. Readers are cautioned not to place undue reliance on these forward-looking statements, and they should not be relied upon in making purchasing decisions.

THE BEST RUN SAP