



Security Challenges

WITH PAYMENTS

Craig Jeffery, *Strategic Treasurer*

Giancarlo Laudini, *TIS*

Thursday, January 25th, 2018

11:00 AM EST

Today's Presenters

Connect on [StrategicTreasurer.com](https://www.StrategicTreasurer.com)   



Craig Jeffery, CCM, FLMI

Founder & Managing Partner
Strategic Treasurer

Craig Jeffery formed Strategic Treasurer LLC in 2004 to provide corporate, educational, and government entities direct access to comprehensive and current assistance with their treasury and financial process needs. His 20+ years of financial and treasury experience as a practitioner and as a consultant have uniquely qualified him to help organizations craft realistic goals and achieve significant benefits quickly.



Giancarlo Laudini

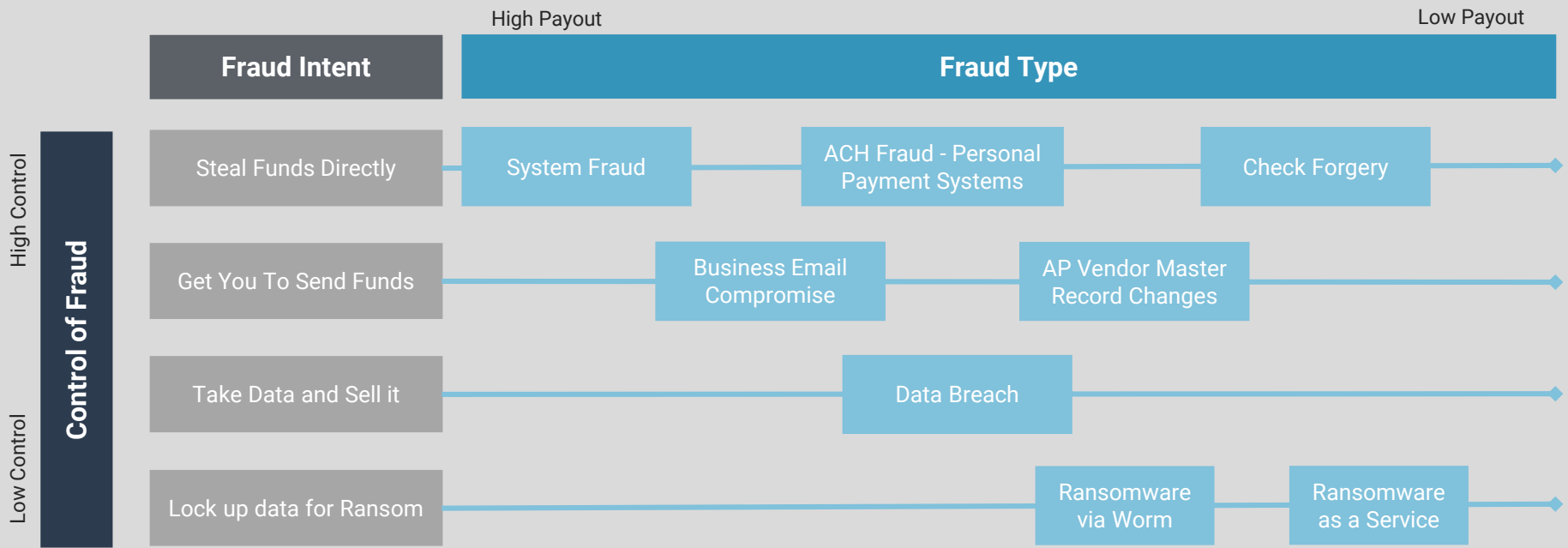
Senior Vice President Global Sales & Marketing Operations
TIS

Giancarlo Laudini, responsible for Global Sales & Marketing Operations at TIS, SWIFT Partner Management and TIS Global Partner Program, is a domain and product expert in the Payments, Bank Connectivity, Bank Account Management arenas as the SaaS (on-Demand) Services. With a strong multi-cultural knowledge, he has been in the IT industry for over 20 years gaining international experience in Cash Management, Electronic Banking and strategic involvement in Global Payment Factory projects for large Multinational Clients.

The Criminal's Playbook

Connect on [StrategicTreasurer.com](https://www.StrategicTreasurer.com)   

The Criminal's Playbook: Fraud Types & Associated Intentions

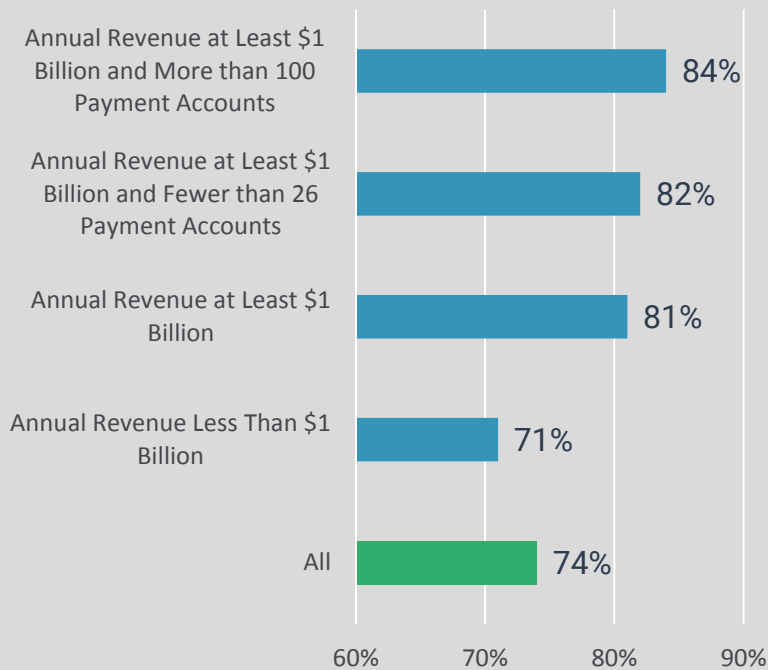


Surveying the Field: There are a wide variety of fraudulent methods for criminals to select from. If an organization is protected at one juncture, a criminal may move on to target them through another avenue or area of exposure. Due to the ever-evolving playbook of today's criminal, organizations must be constantly monitoring their operations to locate exposures and identify suspicious activity.

Overall Fraud Experience in Treasury

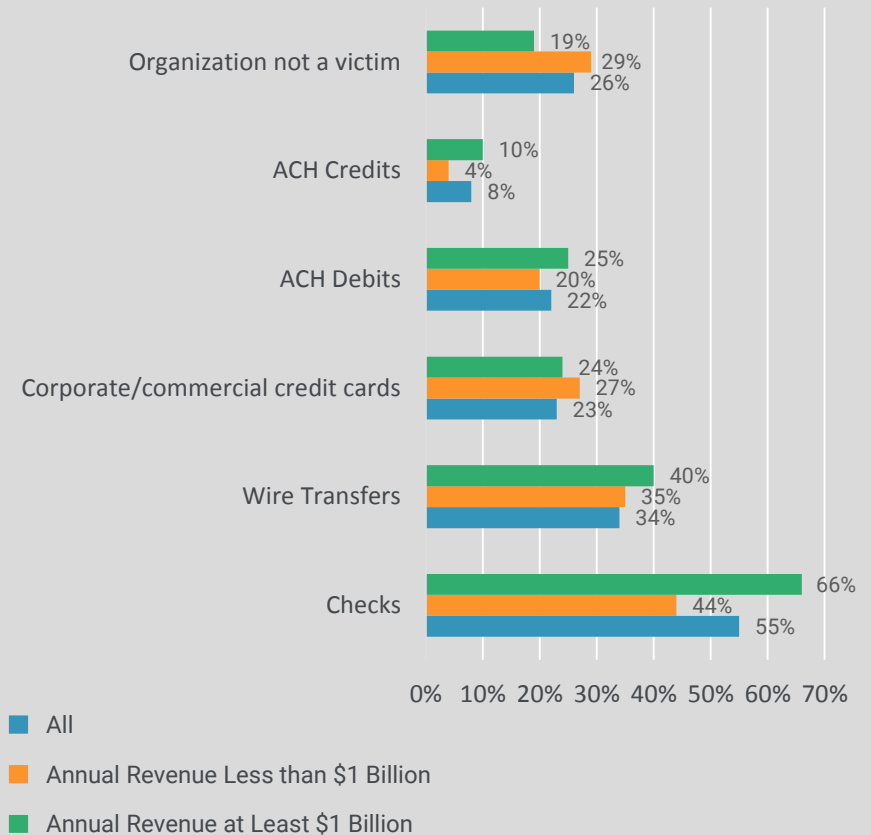
Connect on StrategicTreasurer.com   

Percent of Organizations that Experienced Attempted and/or Actual Payments Fraud in 2016



Source: 2017 AFP Payments Fraud & Control Survey

Payment Methods that were Targets of Attempted and/or Actual Payments Fraud in 2016



Source: 2017 AFP Payments Fraud & Control Survey

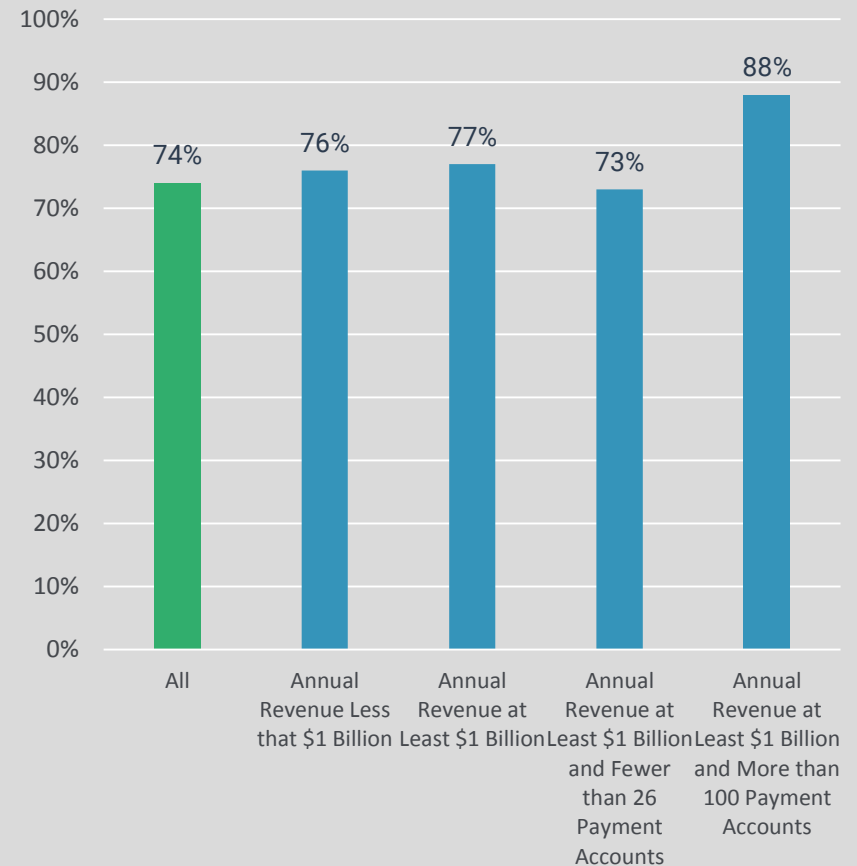
Challenge: Compromised Credentials

Connect on [StrategicTreasurer.com](https://www.StrategicTreasurer.com)   

BEC / Imposter Fraud

- Employee credentials, especially those of high-profile executives or those with authority over payment activity, are a primary target for criminals.
- As treasury is commonly at the helm of an organization's payment operations, their credentials/information are regularly targeted.
- A top method through which these attacks are carried out is BEC schemes, where employees' email credentials are hacked and used to initiate or request fraudulent wire transfers.
- These hacks usually take place through phishing emails or scams. Once an employee clicks on the email or a link in the email, malicious software is spread onto their computer that can track keylogging and assume control of email accounts.
- In 2017, an AFP survey found that 74% of organizations were targeted by BEC scams in the previous year (2016).

Percent of Organizations that Experienced Attempted and/or Actual Business Email Compromise in 2016



Source: 2017 AFP Payments Fraud & Control Survey

Solution: Multi-Factor Authentication

Connect on [StrategicTreasurer.com](https://www.StrategicTreasurer.com)   

Multi-Factor Authentication Explained

- To protect against unwarranted breaches, treasury personnel can protect themselves by requiring multiple levels or layers of authentication.
- This could include the use of passwords, tokens or key fobs, etc. that are each required for an employee to sign into a network or system.
- This makes it more difficult for a criminal to successfully infiltrate an employee's account, as they must be in possession of both a password and a physical token or key fob.
- Multi-factor authentication is crucial in thwarting BEC attacks, as even if employee credentials are jeopardized, the physical token remains in their possession.

Layers of Multi-Factor Authentication



Something an individual **knows**, such as a password or personal fact. This is usually the first layer of authentication employed by firms/treasury.



Something an individual **has**, such as a token or cell phone. The use of a key fob or USB is an example of this.



Something the individual **is**, such as a fingerprint, voiceprint, retinal scan, or other biometrics. These are increasingly being used by banks and are seeing greater adoption in other facets of the industry.



Something the individual **does**, such as the time of day they log in or the IP address they use. This form of user monitoring can be used to identify anomalous behavior before payments are stolen.

AFP Essentials of Treasury Management 5th Edition

Challenge: Insider Fraud, Rogue Employees

Connect on [StrategicTreasurer.com](https://www.StrategicTreasurer.com)   

Unchecked Authority Over Payment Activity

- Treasury personnel with full authority over payment activity or sole ownership of BAM functions may be able to manipulate protocols to transfer company funds to their own accounts.



Unsecured Passwords, Credentials, or Tokens

- If treasury staff have passwords or tokens stored insecurely in a desk drawer or jotted down in a notebook on their desk, they expose themselves to the potential for credentials to be obtained and exploited by other employees for their own personal gain.



Solution: Dual Controls & Segregation of Duties

Connect on [StrategicTreasurer.com](https://www.StrategicTreasurer.com)   

Unchecked Control Over Payment Activity

Recommended practices to prevent embezzlement of funds by treasury personnel include:

- Implementation of dual controls / segregation of duties for all payments generated. This will ensure that no single employee is able to singlehandedly initiate and approve payments.
 - (i.e. One employee initiates payments and another employee approves them.)
- Implementing recurring background checks on current employees. Sometimes, issues that appear in these checks can alert management to potential causes for an employee to commit fraud.
- Implement user monitoring systems that can identify suspicious behavior.

Unsecured Passwords, Credentials, or Tokens

There are several easily-employed practices treasury can utilize to protect against these types of breaches:

- Concept of least privilege.
 - Employees have access to only the information they need for ongoing operations.
 - This means bank account / vendor information is kept confidential except to those who must have access for daily operations.
 - As soon as an employee no longer needs access to confidential information, their access should be revoked.
- Locking passwords & tokens.
 - Passwords, if written down, should be stored in a locked safe or drawer, along with any USBs or other tokens used for initiating payments.
 - A password is no good if its available to everyone.

Challenge: Cyber Breaches

Connect on [StrategicTreasurer.com](https://www.StrategicTreasurer.com)   

Treasury's Cyber Concerns

- Due the rising threat of cyber fraud, companies have indicated elevated concern regarding the safety of their networks, systems, and e-processing operations.
- As payment operations are increasingly conducted electronically, the opportunities for cyber fraud are increased.
- Treasury must understand the full payment operations lifecycle and understand where the weaknesses/exposure points lie.
- Regarding cyber fraud, the following areas are of primary concern for treasury:
 - Internal Networks & Servers
 - Internal Systems (ERP)
 - Third Party Relationships (i.e. banks)
 - Outsourced services (TMS, TMRS, SaaS)

Developing a Control Framework

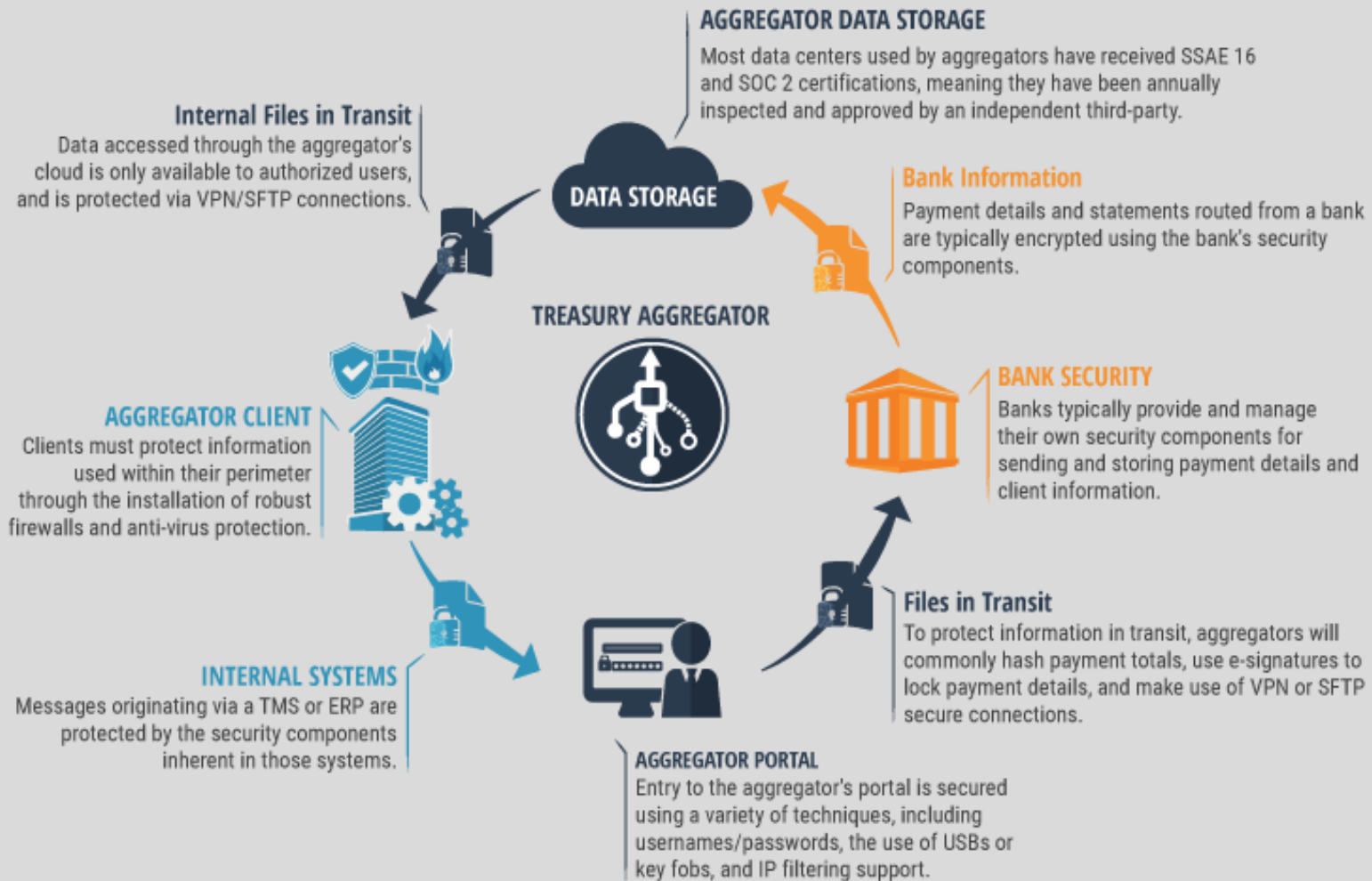
- As cyber fraud can be initiated at multiple points throughout the payments process, treasury must construct a multi-tiered framework to prevent it.
- This involves adopting security standards and practices that protect different segments of the payments process.
- Suggested controls include:
 - Regular employee training / education
 - Elaborate data protection policies
 - Internal System Monitoring
 - External System Monitoring (via a 3rd party)
 - Updated firewalls and antivirus
 - Use of SFTP/VPN Connections when sharing information

A holistic view of a sample security framework and controls are highlighted further on the subsequent slide.

Solution: Security at Every Juncture

Connect on StrategicTreasurer.com   

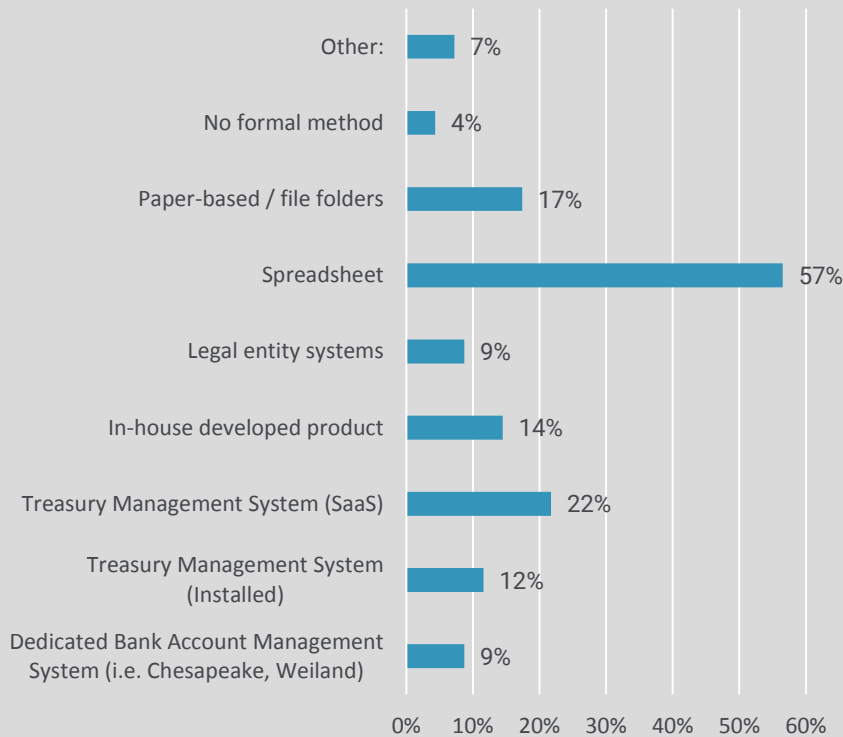
SECURITY FRAMEWORK: TREASURY AGGREGATORS



Challenge: Updating Signer Lists & Managing Accounts

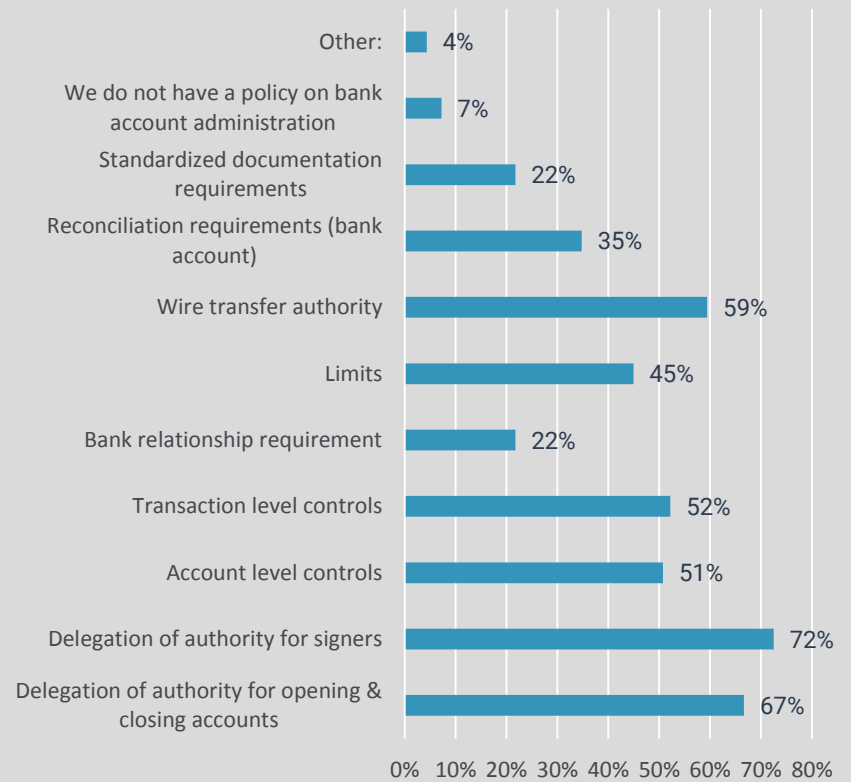
Connect on [StrategicTreasurer.com](https://www.StrategicTreasurer.com)   

How do you currently track your bank account administration - account information, addresses, signers, etc?
(Select all that apply)



Source: 2017 Strategic Treasurer Compliance Survey

Which of the following does your bank account administration policy include?
(Select all that apply)



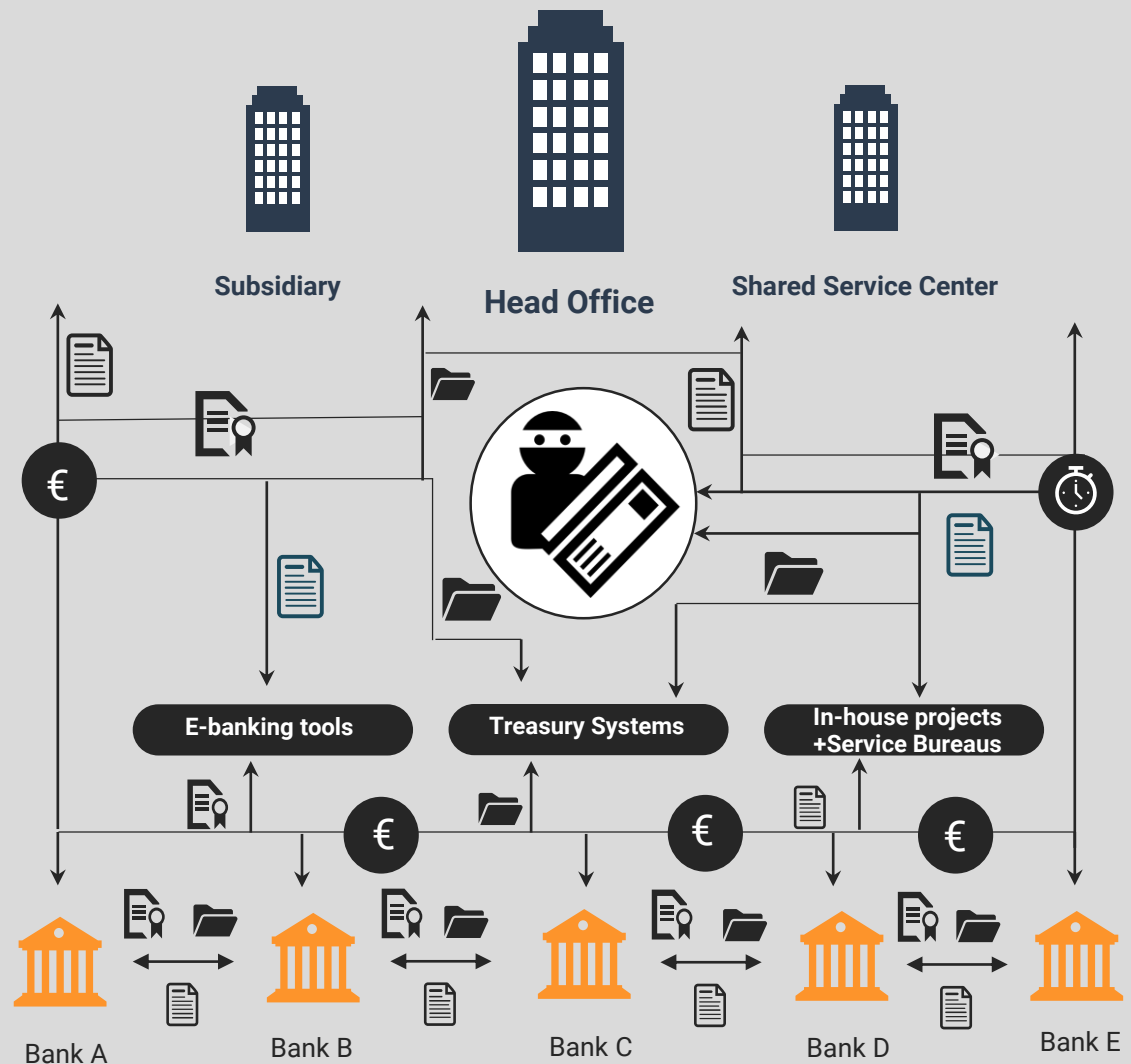
Source: 2017 Strategic Treasurer Compliance Survey

Challenge: Updating Signer Lists & Managing Accounts

Connect on [StrategicTreasurer.com](https://www.StrategicTreasurer.com)   

An Unorganized State

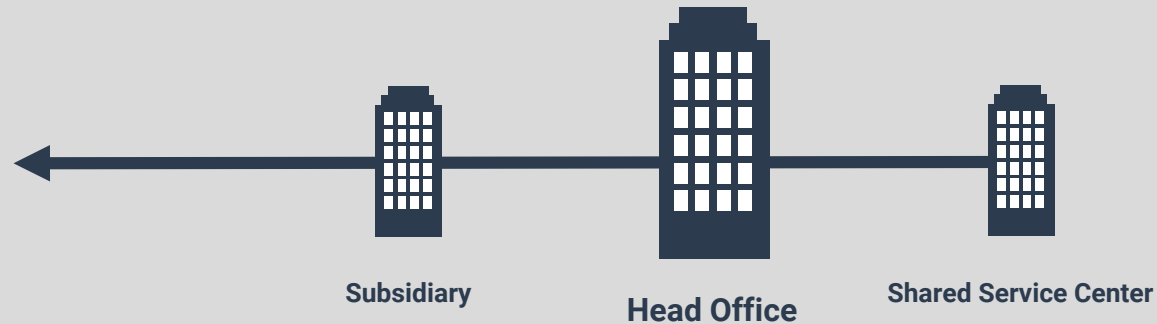
- For a multinational organization with multiple subsidiaries and a large spread of banks, an effective BAM approach is vitally important.
- However, without the proper infrastructure, the process of managing signers and opening/closing accounts will be fragmented.
- Different subsidiaries/branches may be tracking their own signers and accounts internally, but central treasury might not have complete visibility into the process.
- This fragmented approach opens up the door for fraud, especially if accounts that should be closed are left open, and outdated signers that should be removed are left as authorized.



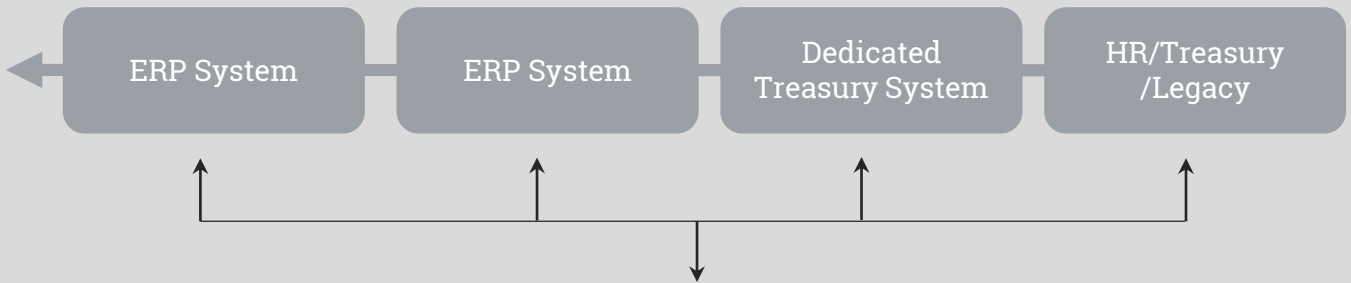
Solution: Integrated BAM Functionality

Connect on [StrategicTreasurer.com](https://www.StrategicTreasurer.com)   

Branch Level
Typically, organizations that experience complications bank account management are attempting to track signers and accounts across multiple locations, subsidiaries, and service centers.



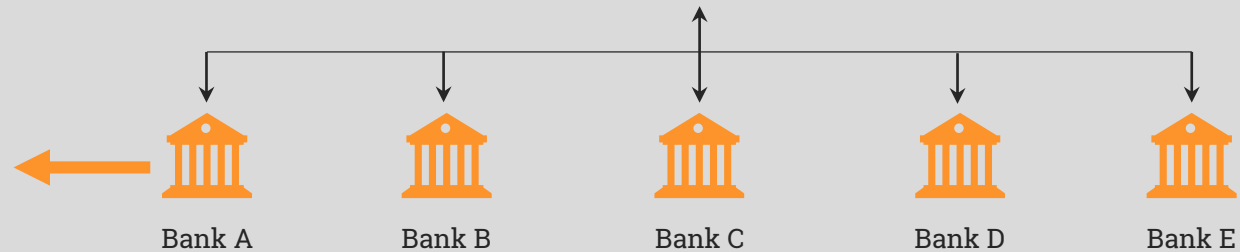
System Level
Specific ERP or TMS systems may have built-in BAM functionality as well, which typically covers all the signers/accounts under its jurisdiction. These solutions may be linked to other BAM solutions for centralized management.



Integrated Solution
Signers and accounts can be aggregated by specific system and bank within the solution. Workflows for signers and accounts can be individually assigned by bank and by the end-user.



Bank Level
Banks typically maintain BAM functionality for their own purposes, and may offer services to clients that cover accounts/signers linked to that specific bank.



Challenge: Identifying Anomalous Payments

Connect on [StrategicTreasurer.com](https://www.StrategicTreasurer.com)   

Speed Matters. For criminals, the faster a fraudulent payment can be pushed through corporate controls and into their bank, the quicker they can make away with the funds.

Biding their Time. Often, a criminal will wait until a holiday or a time when most employees are out of the office before initiating fraudulent transactions, in hopes that they will not be noticed until the funds have already been stolen.

Defensive Posture. Adversely, the faster an organization can identify suspicious activity or payments, the better chance they have at stopping criminals.

Rapid Reconciliation. For firms with high daily payment volumes, the ability to auto-reconcile payments through a TMS or other solution can provide an advantage in quickly identifying errant payments and suspicious activity.



Grab and Run. The goal of criminals is to move funds to their accounts and disappear as quickly as possible.

The Stakes are High. The dollar value of fraudulent funds initiated by criminals can reach millions of dollars in a single attempt.

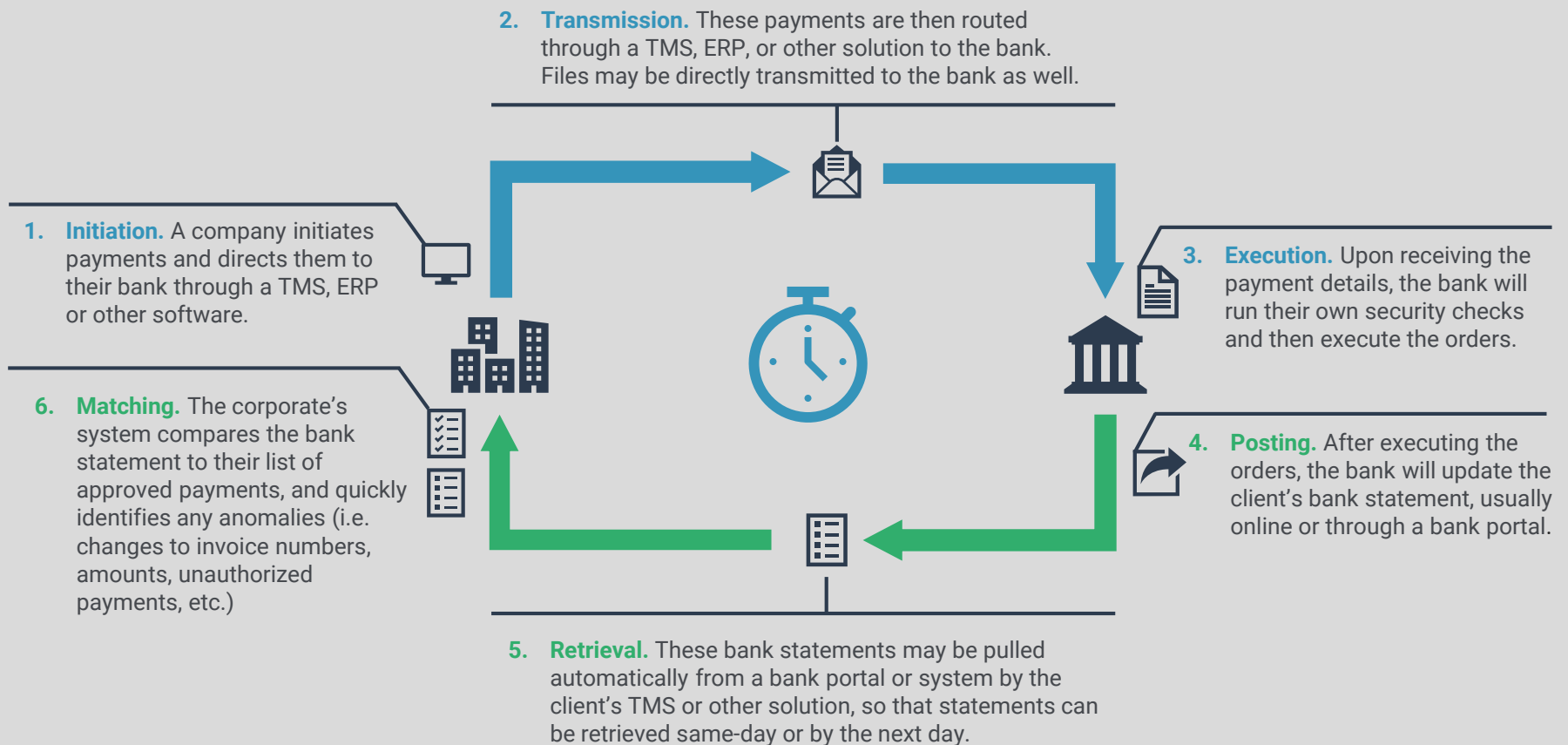
On the Alert. If treasury is to stop fraud activity before a loss occurs, they must be quicker than the criminals in identifying a fraudulent payment and halting the transaction.

Solution: Auto-Reconciliation & Matching

Connect on [StrategicTreasurer.com](https://www.StrategicTreasurer.com)   

The Payments Process: Speed Matters

- The below illustration highlights a typical e-payments workflow. The speed at which the latter half of the workflow, from the bank's posting of a statement to the retrieval and matching of the statement to the corporate's records, is vital for quickly identifying anomalous payments and reversing or freezing the flow of fraudulent funds.



Solutions in Payment Security: Case Study DACHSER SE

Connect on [StrategicTreasurer.com](https://www.StrategicTreasurer.com)   

Company
DACHSER SE



Headquarters
Germany



Industry
Logistics



Products and Services
Transport



Employees
27.450



Revenue
>US\$ 5.7 billion

Objectives

- Harmonization of payment processes in connection with SAP usage
- Reduce governance and security risks
- Straight-through processing including decentralized electronic signature

Challenges

- High costs and inefficient work due to manual intervention in the payment runs between SAP and the heterogeneous bank landscape
- Excel-based reporting systems with high error level and imprecision
- Complexity due to bank formats, decentralized accounting and local release and signature authorizations
- Compliance and audit risks
- No integration of bank communication and reporting systems

Benefits

- End-to-end solution covering all the requirements of automated payment processing: formatting, connectivity and processing of electronic authorizations
- No need to customize bank formats in SAP
- SEPA Compliance

Solutions in Payment Security: Heidelberger Druckmaschinen

Connect on [StrategicTreasurer.com](https://www.StrategicTreasurer.com)   

Company
Heidelberger Druckmaschinen



Headquarters
Germany



Industry
Printing



Products and Services
Printing Machines



Employees
12.500



Revenue
>US\$ 2.5 billion

Objectives

- Replacement of the existing system
- Central control and automation of global payments
- Increased transparency over payment transactions and bank account authorizations
- Straight-Through-Processing achieved by complete SAP ERP integration
- Better management of corporate liquidity
- Automated distribution of bank statements

Challenges

- Lack of transparency and control over foreign payments of local subsidiaries
- Lack of transparency and control over banking authorities
- High effort for the establishment of new and the administration of existing banking interfaces
- Manual effort due to the lack of SAP ERP integration

Benefits

- Transparency, traceability and control of all payments
- Real-time status overview over all payments transactions
- Central overview and control over bank accounts and signatory authorizations
- Security and compliance
- Increase in efficiency and cost benefits
- Rapid implementation and low maintenance costs

Final Thoughts

Key Takeaways for Treasury:




- Fraud continues to be carried out against organizations in high numbers and through a variety of techniques.
- As these trends continue, treasury has become a primary target for criminals, due to their authority over payment operations and access to confidential information such as bank accounts, payment systems, etc.
- In order to protect themselves, treasury must continue to monitor their operations and identify any shortcomings in processes that could open the door for fraudulent schemes.
- Key areas of vulnerability highlighted through industry research includes lack of sufficient firewalls/antivirus, inefficient outdated bank account management features, infrequent reconciliation procedures.
- Ensuring that your organization's coverage in each of these areas will help shore up additional exposures and protect all outlets against breaches, both internally and externally.


Contacts & Training Resource

Connect on [StrategicTreasurer.com](https://www.StrategicTreasurer.com)   

Speaker Contacts

 Craig Jeffery, CCM, FLMI
Founder & Managing Partner
Strategic Treasurer

Email: craig@strategictreasurer.com
Direct: +1 678.466-2222

 Giancarlo Laudini
Senior Vice President Global Sales & Marketing Operations
Treasury Intelligence Solutions (TIS)

Email: giancarlo.laudini@tis.biz
Direct: +49 6227 69824 55
www.tis.biz

Training Course



EMPLOYEE TRAINING
TREASURY SECURITY
ONLINE VIDEO COURSE

TRAINING · TESTING · DOCUMENTATION
Persistent · Updated · Subscription-Based

SecureTreasury™ IGNORING THE THREAT IS **NOT AN OPTION**

Learn more at [SecureTreasury.com](https://www.SecureTreasury.com)

Thank you for participating in this event!