Leveraging technology to prevent fraud and cybercrime

Bob Stark
Vice President, Strategy
Fraud is a driving concern

- **62%** of organizations have experienced attempted or actual payments fraud\(^1\)
- **34%** of organizations have been subjected to a cyberattack in the last 18 months\(^2\)
- **20%** of corporates report fraud committed by employees\(^3\)
- **92%** of Treasurers think they are ‘performing well’ in their battle against fraud\(^4\)
- **Average = 18 months** before fraud detected\(^5\)

Sources: (1, 2, 3) AFP, 2015; (4) ACT, 2016; (5) ACFE, 2014
CFOs and Treasurers need to ask…

- Can connectivity be compromised?
- Do I have visibility into every payment? Are my controls consistent for every bank, every region, every person? Do I review my ACKs?
- Are there controls to prevent unauthorized change to supplier payment info?
- Do I use payment watchlists?
- Do I have a control center to view all transactions and modifications?
- Do I review my ACKs?
- How many bids before a trade? Can Settlement Instructions be modified?
- How many layers of protection exist after your password?
- How many layers of protection exist after your password?

Fraud & Cybercrime in Treasury
Fraud Prevention

Spear Phishing

- Cybercriminals are specifically targeting...you
- Attacks are quick and lethal; one mistake or exception from policy is all that it takes
- Typically hack your system or convince you to do something
Application Security – Protecting access to your system

- UserID/Password should not grant access to the system
- Attacks prey on weak login/authentication – the easiest entry point to hack a software solution and access data
- Require combination of password controls:
  - Password timeouts, resets, history, alphanumeric requirements
  - Virtual Keypad
  - Multi-factor authentication (hard or soft token)
  - IP Filtering
  - Single Sign-On w/ internal IT environment
Fraud Prevention – Spear Phishing

Getting you to do their dirty work

- Business email compromises (BEC) the most popular
- Changing payment instructions is another favorite
- Attacks prey on lack of formal change management process
Data Security

- IT thinks treasury data is safer hosted externally
- Cloud technology offers more safeguards than internal hosting
  - Encryption of data - in transit and at rest
  - Hosting within audited certified data centers that feature 24/7 security, biometric access
  - Separation of duties & other policy driven protections to restrict access to hosting infrastructure and client data
  - Firewalls to protect externally and between tiers
Fraud Prevention – Data Compromise

Assessing Data Security - Audit Reporting

- Most vendors offer a SOC1 Type II report
- IT often requests a SOC2 Type II report
- Must evaluate details of audit; there is no pass/fail

<table>
<thead>
<tr>
<th>Report</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SOC1 (SSAE16)</td>
<td>SOC1 is the report; SSAE16 is the standard SSAE16 is AICPA’s ‘minimum standard’</td>
</tr>
<tr>
<td>SOC2</td>
<td>AICPA’s recommended report for cloud service providers due to standardized Trust Service Principles</td>
</tr>
<tr>
<td>Penetration Testing</td>
<td>Most vendors outsource to specialists (Intel, Qualys, etc.)</td>
</tr>
</tbody>
</table>
Is my bank connectivity safe?

- Recent hacking of payments software has shaken the industry
- Concerns arise about controls surrounding the access points
- Two easy solutions:
  1) Communication to/from banks must be encrypted; no human readable files!
  2) Ensure safeguards of hosted connectivity and service bureaus meet your organization’s information security
Fraud Prevention – Bank Accounts

Control of Bank Accounts

- As organizations expand/decentralize, easy to lose control of accounts and signatories
- Need to establish:
  1) Central repository – visibility into accounts, tracking of authorized signers, and one source for documentation
  2) Structured workflows – mandate approval processes to ensure no ‘under the radar’ bank accounts or signatories
  3) Reconciliation procedures – with the bank(s)
Fraud Prevention – Payments
Fraud Prevention – Payments

- Each exposure point → opportunity for cybercrime
- Exceptions to standardized process → opportunity
- Good news: there are good ways to protect!

Exposure Points: Must be protected
Separation of duties and application of limits are key; Ensure approvals align with dollar limits

Standardization of approval workflow across all banks and all payment types is important – e.g. mandate review of attached documentation
Payment files to bank must be encrypted
Acknowledgements/confirmations must be reviewed
Where available, apply digital signatures (e.g. SWIFT 3SKey) to authenticate exported payment files
Review payments vs. sanctions lists (e.g. OFAC)
Trading – settlement instructions

- Standard settlement instructions (SSI) avoid redirection of funds to unauthorized accounts
  - Payment template should be automatically attached to trade and require approval to edit/remove
  - Even harder to audit disparate trading/payment workflows (e.g. initiate trade / walk paper down the hall / initiate payment)
Fraud Prevention – Trading

Trading – making the right trade

- More of an enforcement, than prevention
  - Trade has already occurred when it shows in treasury system

- Use of approvals and limits will help enforce the right behavior
  - Even if you shouldn’t have done it, you still have to approve it after

- Also tracking multiple bids per trade is helpful to ensure right bid was selected
  - Also necessary for Dodd-Frank (for the exact same reason)
From prevention....to detection
**Fraud Detection**

**Identifying Fraudulent Transactions**

- Review of audit trails will identify specific actions

![Audit trail - (Referential audit trail - Accounts)](image)

<table>
<thead>
<tr>
<th>Entity type</th>
<th>Entity code</th>
<th>Entity number</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AD - Define dual administration</td>
<td>Signatory Management-Admin</td>
<td>350544888</td>
<td>Modification</td>
<td></td>
</tr>
<tr>
<td>AD - Define dual administration</td>
<td>Signatory Management-Admin</td>
<td>350544882</td>
<td>Modification</td>
<td></td>
</tr>
<tr>
<td>AD - Define dual administration</td>
<td>Signatory Management-Admin</td>
<td>350544884</td>
<td>Modification</td>
<td></td>
</tr>
<tr>
<td>AD - Define dual administration</td>
<td>Signatory Management-Admin</td>
<td>350544886</td>
<td>Modification</td>
<td></td>
</tr>
<tr>
<td>AD - Define dual administration</td>
<td>Signatory Management-Admin</td>
<td>350544888</td>
<td>Modification</td>
<td></td>
</tr>
<tr>
<td>AD - Define dual administration</td>
<td>Set-up Account</td>
<td>350544867</td>
<td>Modification</td>
<td></td>
</tr>
<tr>
<td>AD - Define dual administration</td>
<td>Set-up Account</td>
<td>350544867</td>
<td>Modification</td>
<td></td>
</tr>
<tr>
<td>AD - Define dual administration</td>
<td>Set-up Account</td>
<td>350544867</td>
<td>Modification</td>
<td></td>
</tr>
<tr>
<td>AD - Define dual administration</td>
<td>Set-up Account</td>
<td>350544867</td>
<td>Modification</td>
<td></td>
</tr>
<tr>
<td>AD - Define dual administration</td>
<td>Set-up Account</td>
<td>350544867</td>
<td>Modification</td>
<td></td>
</tr>
<tr>
<td>AD - Define dual administration</td>
<td>Set-up Account</td>
<td>350544867</td>
<td>Modification</td>
<td></td>
</tr>
<tr>
<td>AD - Define dual administration</td>
<td>Set-up Account</td>
<td>350544867</td>
<td>Modification</td>
<td></td>
</tr>
<tr>
<td>AD - Define dual administration</td>
<td>Set-up Account</td>
<td>350544867</td>
<td>Modification</td>
<td></td>
</tr>
<tr>
<td>AD - Define dual administration</td>
<td>Set-up Account</td>
<td>350544867</td>
<td>Modification</td>
<td></td>
</tr>
<tr>
<td>AD - Define dual administration</td>
<td>Set-up Company</td>
<td>350544878</td>
<td>Modification</td>
<td></td>
</tr>
<tr>
<td>AD - Define dual administration</td>
<td>Set-up Company</td>
<td>350544878</td>
<td>Modification</td>
<td></td>
</tr>
<tr>
<td>AD - Define dual administration</td>
<td>Set-up Company</td>
<td>350544878</td>
<td>Modification</td>
<td></td>
</tr>
<tr>
<td>AD - Define dual administration</td>
<td>Set-up Company</td>
<td>350544878</td>
<td>Modification</td>
<td></td>
</tr>
<tr>
<td>AD - Define dual administration</td>
<td>Signatory Management-Sign category</td>
<td>350544879</td>
<td>Modification</td>
<td></td>
</tr>
<tr>
<td>AD - Define dual administration</td>
<td>Signatory Management-Sign category</td>
<td>350544879</td>
<td>Modification</td>
<td></td>
</tr>
<tr>
<td>AD - Define dual administration</td>
<td>Signatory Management-Sign category</td>
<td>350544879</td>
<td>Modification</td>
<td></td>
</tr>
<tr>
<td>AD - Define dual administration</td>
<td>Set-up Bank</td>
<td>708212398</td>
<td>Modification</td>
<td>Bank Connections</td>
</tr>
<tr>
<td>SU - Process template</td>
<td>BANK_CONN</td>
<td>752736465</td>
<td>Modification</td>
<td>Bank Connections</td>
</tr>
<tr>
<td>SU - Process template</td>
<td>BANK_CONN</td>
<td>752736465</td>
<td>Modification</td>
<td>Bank Connections</td>
</tr>
<tr>
<td>SU - Process template</td>
<td>BANK_CONN</td>
<td>752736465</td>
<td>Modification</td>
<td>Bank Connections</td>
</tr>
<tr>
<td>SU - Process template</td>
<td>BANK_CONN</td>
<td>752736465</td>
<td>Modification</td>
<td>Bank Connections</td>
</tr>
<tr>
<td>SU - Process template</td>
<td>BANK_CONN</td>
<td>752736465</td>
<td>Modification</td>
<td>Bank Connections</td>
</tr>
<tr>
<td>SU - Process template</td>
<td>BANK_CONN</td>
<td>752736465</td>
<td>Modification</td>
<td>Bank Connections</td>
</tr>
<tr>
<td>SU - Process template</td>
<td>BANK_CONN</td>
<td>752736465</td>
<td>Modification</td>
<td>Bank Connections</td>
</tr>
<tr>
<td>SU - Process template</td>
<td>BANK_CONN</td>
<td>752736465</td>
<td>Modification</td>
<td>Bank Connections</td>
</tr>
<tr>
<td>SU - Process template</td>
<td>BANK_CONN</td>
<td>752736465</td>
<td>Modification</td>
<td>Bank Connections</td>
</tr>
<tr>
<td>File alert</td>
<td>OFX_ALERT</td>
<td>777972138</td>
<td>Creation</td>
<td>Cash Flow Upload</td>
</tr>
<tr>
<td>File alert</td>
<td>OFX_ALERT</td>
<td>777972138</td>
<td>Creation</td>
<td>Cash Flow Upload</td>
</tr>
<tr>
<td>File alert</td>
<td>OFX_ALERT</td>
<td>777972138</td>
<td>Creation</td>
<td>Bank Statement Upload</td>
</tr>
<tr>
<td>File alert</td>
<td>OFX_ALERT</td>
<td>777972138</td>
<td>Creation</td>
<td>Bank Statement Upload</td>
</tr>
</tbody>
</table>
Fraud Detection

Identifying Fraudulent Transactions

- Daily monitoring of balances and transactions will find suspicious/fraudulent transactions:
  - Daily bank reporting will proactively find suspicious transactions; especially via use of dashboards and automated reporting
  - Daily cash positioning forces review of transaction variances
  - Monthly accounting reconciliation offers same ability, but another checkpoint
Identifying Fraudulent Transactions

- Separating GL Posting from GL Reconciliation
  - Processes should be separated
  - Same person that created journal entries should not be reconciling those entries
  - Implementing both workflows in same system makes it easier to prove to auditors proper controls are in place
Central Monitoring

- Payments to be transmitted to bank
- Internal workflow changes (e.g. limits and approvals)
- Bank Accounts & Signatories
- Daily monitoring & reconciliation of all transactions
CFOs and Treasurers need to ask...

- Can connectivity be compromised?
- Do I know my account signatories? Who can change them? Does my bank have the same list?
- How many bids before a trade? Can Settlement Instructions be modified?
- How many layers of protection exist after your password?
- Do I have visibility into every payment? Are my controls consistent for every bank, every region, every person? Do I review my ACKs?
- Are there controls to prevent unauthorized change to supplier payment info?
- Do I use payment watchlists?
- Do I have a control center to view all transactions and modifications?
CFOs and Treasurers have answers

- Fraud & Cybercrime in Treasury
- Bank Account Mgmt
- Investments & Trading
- Access to Treasury Technology
- Payments
- Supplier Account Verification
- Fraud Detection
- Connectivity

- Encrypted communications
- IT Evaluation of connectivity-as-a-service provider
- Single system of record
  - Controls for changes to bank data
  - Full visibility to monitor activity
- Recorded multiple bids
  - Standard Settlement Instructions
- Multi-factor authentication!
  - + IP Filtering, VPN, SSO, V-keyboard
  - Applied for business continuity
- Separation of duties and multi-approvals
  - Standardized Controls and Processes
  - Digital Signatures
- Standardized review/approval of changes to supplier bank instructions
- Watchlist filtering for payments
  - Overall visibility into audit, controls, activity

Fraud & Trading
- Bank Account Mgmt
- Investments & Trading
- Access to Treasury Technology
- Payments
- Supplier Account Verification
- Fraud Detection
- Connectivity

- Encrypted communications
- IT Evaluation of connectivity-as-a-service provider
- Single system of record
  - Controls for changes to bank data
  - Full visibility to monitor activity
- Recorded multiple bids
  - Standard Settlement Instructions
- Multi-factor authentication!
  - + IP Filtering, VPN, SSO, V-keyboard
  - Applied for business continuity
- Separation of duties and multi-approvals
  - Standardized Controls and Processes
  - Digital Signatures
- Standardized review/approval of changes to supplier bank instructions
- Watchlist filtering for payments
  - Overall visibility into audit, controls, activity

© 2016 Kyriba Corp. All rights reserved.
Questions?

Bob Stark
bob.stark@kyriba.com
@treasurybob