STANDARDS BOARD FOR ALTERNATIVE INVESTMENTS

# Cash Handling and Cyber-security

SBAI Toolbox

## Introduction

Cyber-crime is an ever-increasing, evolving threat to organisations of all sizes. As investment managers routinely engage in the transfer of large sums of money in their daily business activities, they are attractive targets for a spectrum of cyber-frauds. The regularity of these transfers (either within a fund structure or to external vendors) can result in a decreased awareness of the risks surrounding the transactions increasing the vulnerability to cyber-attacks.

Historically, controls investment managers have put in place for these transfers have focused on preventing internal fraud but, many of these controls do not provide adequate protection from cyber-attacks and external fraud. In particular with the current and expected continued rise in remote working, appropriate controls to safeguard transactions against a wide range of threats (including cyber-crime) become more important than ever as employees working outside an office environment may lower their guard against these threats. This has been highlighted by many regulators including the Hong Kong SFC in a circular in April 2020[1].

The purpose of this memo is to provide practical advice and guidance to alternative investment firms and institutional investors. Managers will be able to use this guidance to benchmark their current processes and investors will be able to use this to guide their due diligence. Specifically, this SBAI Toolbox memo covers the following areas:

1. Overview of the Threat Environment
2. Common Types of Cyber-fraud
3. Common Cyber-fraud Techniques
4. Controls to Mitigate the Risk (including guidance on due diligence questions that investment managers should be asking their fund administrators[2] and other strategic financial partners)

The memo also contains four detailed appendices of illustrations and mini-case studies:

I. Types of Fraud exploiting weaknesses in Cash Controls and Cyber-security
II. Examples of Payment Fraud linked to Cyber-security
III. Illustration of Controls – Electronic Payment System
IV. Illustration of Controls – Non Electronic Payments
V. Illustration of Controls – Investor Payments

---

The SBAI Toolbox is an additional aid to complement the SBAI's standard-setting activities. While alternative investment fund managers sign up to the Alternative Investment Standards on a comply-or-explain basis, the SBAI Toolbox materials serve as a guide only and are not formally part of the Standards or a prescriptive template.

[1] https://www.sfc.hk/edistributionWeb/gateway/EN/circular/intermediaries/supervision/doc?refNo=20EC37

[2] Note than throughout this memo any references to a Fund Administrator can be taken to refer to any third-party service provider that is involved in the payments process for example an outsourced middle or bank office provider.

This memo follows on from the SBAI Cyber-Security Toolbox Memo published in 2019, which can be used as a resource for putting together a cyber-security program.

## Overview Threat Environment

The 2019 Cost of Cybercrime study[3] by Accenture (which surveyed 355 companies in 11 countries across 16 different industries) shows that attacks are getting both more frequent and more expensive and this is before considering the reputational costs.

**11%** increase in the number of security breaches on corporations in one year

**+67%** over five years

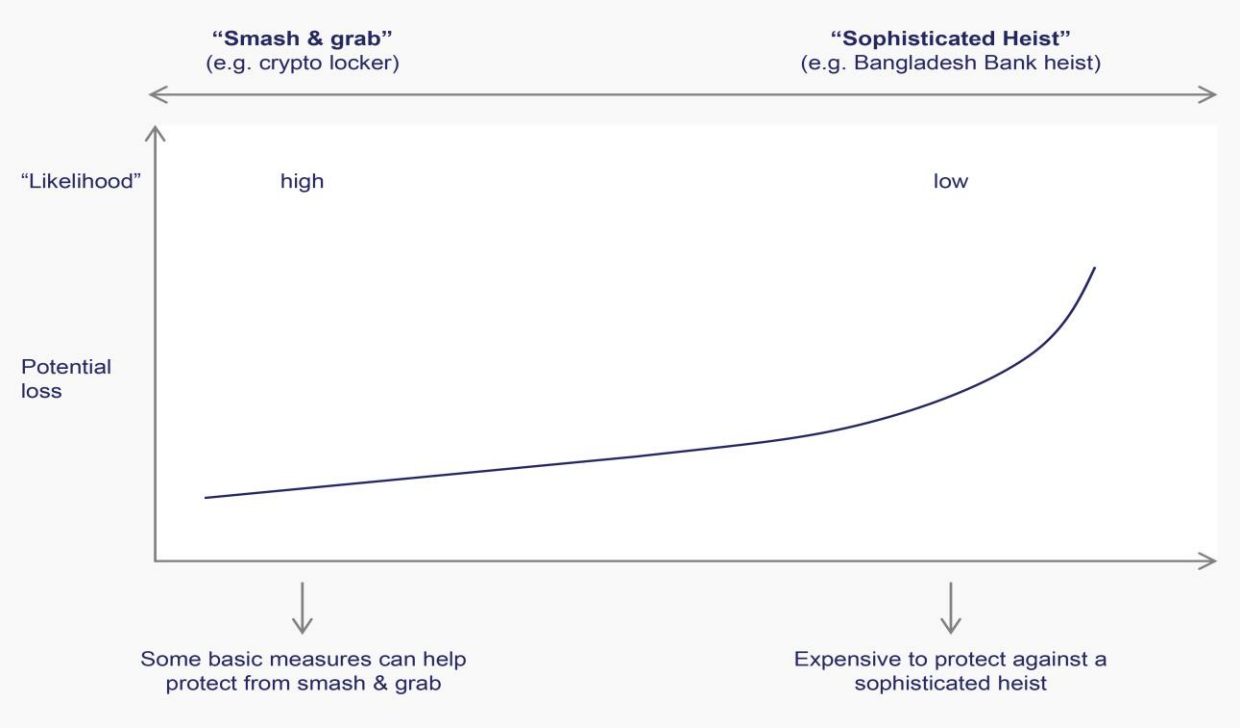
**12%** increase in the average cost of cyber-crime for an organisation

**+72%** over five years

The National Futures Association (NFA) also issued a Notice to Members in May 2020[4] warning of an increase in fraudulent phishing emails that warranted its members vigilance.

### Spectrum of incidents in Asset Management

A spectrum of threats exists, from simple invoice fraud exploiting weaknesses in cash controls to sophisticated attempts to redirect large fund payments such as investor redemptions or capital calls.




[3] https://www.accenture.com/us-en/insights/security/cost-cybercrime-study

[4] https://www.nfa.futures.org/news/newsNotice.asp?ArticleID=5226

## Common Types of Cyber-fraud

As shown in Appendix I, cyber-criminals have successfully targeted a wide range of financial transactions, some of which are generic and some of which are more specific to financial services and alternative investments. The most common types of fraud are:

**Fraudulent Invoice Request**

- A basic, but surprisingly successful technique involves sending in a fake invoice to an organisation, who then settle the outstanding balance and directly pay the attacker
- These attacks can be made more successful using open source research, or access to the victim's email, to research a list of vendors used by the company
- Alternatively, access to senior management's email can be used to 'forward' the invoice internally, often written with an aggressive tone to suggest an employee is at fault for not having previously paid the invoice and suggesting a sense of urgency. Such a tactic may be used to attempt to bypass existing approval processes

**Fraudulent Payment Request**

Like the fake invoice, the attacker requests a new bank transfer is made to an account they control. Often these requests are addressed as from senior management, either through compromised email infrastructure or via spoofed email addresses

Again, the tone and nature of the email will convey a heightened sense of urgency, and serious consequences should the payment not be made on time.

**Change of Payee Details**

Another variation on the above examples is to take an established, approved transaction and attempt to alter the payment details to change the destination bank account. This technique has been observed against all types of payment transactions, including invoices, bank transfers, salary payments and event payments to prime brokers.

These attacks almost always require some level of access to the victim's email infrastructure. This access allows the attacker to find and alter a legitimate transfer instruction, greatly increasing their chance of success. Alternatively, emails may be spoofed to appear as if they are from the party receiving the payment requesting to change the details.

In the UK Financial Conduct Authority's recent publication on insights from their Cyber-Coordination Groups[5], it was highlighted that a future trend will likely see attackers building more advanced capabilities to target payment systems and transactions, making it more important than ever to understand cyber-crime and how to prevent it.

## Common Cyber-fraud Techniques

Cyber-criminals may use more than one of these techniques at any given time. Using information gathered from these techniques, the attacker is able to craft a fraudulent email that likely attempts one of several common frauds, such as changing bank details on a payment, or requesting an urgent new payment to be made. Appendix II contain real life examples of these types of incidents.

### Business Email Compromise (BEC)

Cyber-criminals will almost always initially seek to compromise a company's email system. Common targets for email access are listed below:

[5] https://www.fca.org.uk/publications/research/insights-cyber-coordination-groups#lf-chapter-id-ccg-insights-cyber-risk-emerging-and-future-trends

| Senior Executives (CEO/COO/CFO etc.) | Finance Team | IT Administrators |
|---|---|---|
| Senior executives are heavily targeted since they often have the authority to approve the fraudulent transactions the attacker is attempting to make. | Finance teams are targeted as they may have access to payment systems the attacker is attempting to gain access to. With access to these user's mailboxes, attackers can reset passwords to finance systems and defeat additional security controls which require two-step verification using emailed security codes. | IT administrators are targeted, since privileged access to the email system allows the attacker to take controls of multiple email accounts simultaneously. Through this, attackers can pose as multiple parties and defeat 'four eyes principles', where a transaction must be reviewed and approved by two or more individuals. |

These functions, job titles and names are easily searched on social media, regulatory filings and other open-source materials:

Accessing a user's mailbox is normally achievable because the organisation is not using Multi-Factor Authentication (MFA)[6] to protect the email system. The number of attacks that can bypass MFA are very small, but despite this, many firms remain at risk by not employing this free control. The Singapore MAS included the strengthening of user access controls in the elements that became compulsory from their existing MAS Technology Risk Management Guidelines in 2019[7] highlighting regulatory focus on strong preventative controls.

There are two common actions a cyber-criminal may take once access to the email system has been gained:

- **Information Gathering:** Use email history and old attachments to finely hone a fraudulent email to read identically to a genuine email from the user. Attachments may also be used to extract signatures and other information used to verify transactions, such as passwords or phrases. Skilled attackers will also set up email rules to automatically delete or move all emails relating to their fraud, out of the victim's inbox. This means a victim could be at their computer, actively using their inbox at the same time the attacker is conducting fraud, completely unaware that anything is wrong.

- **Email Forwarding:** A cyber-criminal may establish "forwarding rules" from an inbox that they have access to that will identify any emails with potentially sensitive terms in the subject (e.g.: "Invoice", "Payment", "Transfer"). These emails will automatically be forwarded from the victim's inbox, to an external email address the attacker controls.Critically, even if the victim realises or suspects their email has been hacked, and changes their password, forwarding rules are not affected. In this way, attackers may have persistent access to a mailbox for months or years, without detection. This allows them to remotely monitor the email of a victim, without needing to repeatedly log in to the victim's email account, reducing their risk of detection.

### Email Spoofing or Impersonation

Where attackers are unable to compromise the company's email system, many attackers choose to send "spoofed" emails which impersonate that user.

[6] Multi-Factor Authentication (MFA) is security feature that requires at least two forms of verification (e.g. password and authentication through a separate app) to either confirm a user's identity or verify a transaction is valid.

[7] https://www.mas.gov.sg/news/media-releases/2019/mas-issues-new-rules-to-strengthen-cyber-resilience-of-financial-industry

There are different ways to impersonate an email address, but the most common is for the attacker to register a similar looking domain to the legitimate domain they are attempting to copy. Common approaches are to registered misspellings, such as replacing “m” for “rn”, “w” for “vv” etc.

User training (such as educational phishing campaigns and cyber-security awareness training) can be used to help mitigate this risk, but as spoofing emails become more sophisticated they can be very hard to spot by users without additional technical controls in place to help identify suspicious emails.

## Controls to Mitigate the Risk

There are various controls that can be put into the payment process that will mitigate the risk of both misappropriation of funds and external fraud attempts. Some of these are technical controls, others are processes and procedures. Appendices III, IV and V provide further guidance on how to modify many common processes to make them more resilient against internal and external threats.

Technical controls that should be considered are included below. Those managers who use outsourced managed service providers for their IT should discuss these requirements with their provider:

### Multi-Factor Authentication (MFA)

- MFA should always be used to secure external access to email, where external access is not required it should be disabled except via mobile.
- MFA systems that rely on SMS do have weaknesses (e.g. Sim Cloning) and secure tunnel-based MFA methods are more secure. That said, any type of MFA will be more secure than not having this in place.
- Use MFA to secure payment and approval portals. This should not be configured to use email-based tokens. Where vendors and service providers are issuing tokens for access to these systems, managers should request the shortest possible window for TTL (token timeouts) to prevent any leavers from continuing to have access to accounts after long periods of time.
- Where a firm’s service providers do not provide MFA for access to their systems as a standard offering, managers should apply pressure for this to be adopted.

### Hardware and Software Protections

- Mobile device management (MDM) should be used to limit mobile access to known, approved devices
- Ensure security patches are applied in a timely manner
- Implement threat detection approaches such as anomaly monitoring
- Voice recognition may be used as an additional control to access services. This shouldn’t be relied on as a golden control; however, as there are increasing cases of deep fakes using publicly available recordings of people (the number of these available tends to increase with the seniority of the person)
- URL Filtering can be used to prevent employees from accessing known harmful sites (e.g. sites used for phishing or identified as fraudlent websites).
- Any file transfers with service providers should be encrypted using Secure File Transfer Protocol/SSH File Transfer Protocol (SFTP).

### Single Sign On (SSO)

- SSO should be used wherever possible (alongside MFA).

- SSO helps to mitigate the onboarding/offboarding risks associated with staff turnover as all accounts can be deactivated centrally. This was highlighted in the January 2020 SEC OCIE Cyber-Security Resiliance and Observations report.[8]
- Where SSO cannot be used, ensure your joiners, movers and leavers process is promptly followed for all external accounts on email, payment systems and approval portals. This will prevent ex-employees and cyber-criminals using old accounts to access these systems.

**Email Protections**

- Automated email forwarding outside of the organisation should be disabled, if not required. If required, this should be logged and require approval
- Protect email compliance archives from unauthorised access using MFA and further access controls, as appropriate
- Implement anti-spoofing controls such as DMARC[9]. These free controls can be used to help identify and block spoofed emails. These can also be used to prevent attackers spoofing your domain to your suppliers, investors etc.
- Consider purchasing any domain names that are similar to yours e.g. .com if your company uses .co.uk or vice versa
- Implement email impersonation detection. Most modern email systems have capabilities to detect common variants and misspellings of domains
- Email server communication should be secured using Transport Layer Security (TLS) which encrypts the email message while it is in "transit" from one secure email server to another. This should be discussd and tested with service providers as both parties will be required to use this.

### Actions to Strengthen Common Financial Processes

**Electronic Portals**
Electronic, user-controller, payment portals should be used wherever possible. This is particularly the case for high risk activities such as adding a new payee or changing existing bank details.

**Password Protection**
If using email, password protect email attachments and communicate the password to the recipient by a non-email method (e.g. phone).

**Dual Authorisation**
For confirming settlement instructions, approving and releasing payments, dual authorisation (including senior manager reviews) should be in place at a minimum. Ideally there should be additional reviews for larger amounts.

**Call-Backs**
Call backs to confirm instructions with a person on an authorised signatory list who was not the person that made the instruction should be completed.

**Involvement of an Independent Third Party**
Wherever possible (and at a minimum for external transfers) an independent third party (such as a fund administrator or outsourced middle office provider) should be involved in the payment process.

**Detective Controls**
Regular (ideally daily) reconciliations of cash accounts should be completed to identify any unusual or erroneous activity.

[8] https://www.sec.gov/files/OCIE%20Cybersecurity%20and%20Resiliency%20Observations.pdf

[9] Domain-based Message Authentication, Reporting and Conformance – allows the user to discard untrusted emails and generates reporting on how email is being handled.

Further illustrations on how to strengthen payment processes including use of Fund Administrator controlled accounts, pre-approved SSIs and call-back procedures are contained in Appendices III, IV and V.

### Due Diligence

Use of a third-party administrator (or other independent service provider such as an outsourced middle office) within payment transactions is an effective control in adding an additional independent set of eyes to the process. To make sure this is an appropriate control, investment managers need to ensure that thorough due diligence is completed at the initial onboarding stage and in periodic (ideally at least annual) reviews. The starting point to be able to determine which service providers require detailed due diligence is for the firm to ensure they know all of their vendors, how critical they are, what processes they are involved in and what data they store on their systems. Due diligence should cover:

- Cyber & Information Security Controls – all technical risk mitigants detailed above should be replicated at the administrator. Certifications (e.g. ISO 27001, SSAE18/SOC2 etc.) to ensure the appropriateness and effectiveness of controls should be requested and reviewed, where applicable
- Payment Process Controls – this should include dual authorisations with the appropriate level of seniority, verifications to authorised signatory lists, call-back procedures and user access controls to an electronic payment systems

## **Appendix I -** Types of Frauds exploiting weaknesses in cash controls and cyber-security

The important thing to note about almost all these types of frauds is that direct access to email accounts makes them easier to perpetrate and reduces the amount of legwork required for a single fraud. The first step in any control to prevent cyber-fraud is to ensure that email servers are secure.

| Type | Descriptions | Observations |
|---|---|---|
| Fake capital call notice | Investor receives capital call notice by email, including wrong bank account details | May require knowledge of the investor's allocations; however, allocations from large institutional investors are often made public – particularly for pension funds<br>May require knowledge of agreed process for making investments. Capital call notices delivered via PDF on email are more at risk of this type of attack.<br>May need to pre-empt a capital call that the investor expects; however, may be opportunistic including language around a new deal opportunity or required servicing of an existing investment.<br>Exploits weak overall cash controls and weak cyber-security protections on emails. |
| Fraudulent change of bank account details | Fund Administrator receives (fake) email from investor (or manager) to change underlying bank account details for redemption<br>Investor receives fraudulent email changing bank account details for subscription or capital call | Requires detailed knowledge of the investor name, fund they are invested into and the administrator servicing the fund. Note that with large investors some of this information will be public.<br>There will often be a sense of urgency with this request and pressured follow up until it is completed.<br>May require knowledge of an investor's intent to redeem. This may be public (think of widespread articles in the financial press when large pension funds decide to reduce hedge fund allocations) or may be a long game where they will wait for a redemption to take place. |

| | | |
|---|---|---|
| | Manager receives fraudulent email changing a vendor's bank account details | Exploits weak overall cash controls and weak cyber-security protections on emails. |
| Issuance of Fake Invoice | Fund Administrator or Manager receives a fraudulent invoice for payment | Require knowledge of typical vendors for the Fund. This could be obtained through audited financial statements, articles that Manager employees may have been quoted in promoting services or press releases from companies announcing large managers have started using their products.<br>Exploits weak overall cash controls and weak cyber-security protections on emails.<br>Exploits weak Fund budgeting and invoice approval processes between the Manager and the administrator. |
| Fake requests from Senior Management to transfer money | Employee in the firm receives (fake) email from a senior manager asking for money to be transferred (usually urgently) | Requires knowledge that the senior manager is not in the office. This can often be sourced from things such as LinkedIn (e.g. posting location to secure meetings, advertising attendance of a conference or participating on a panel) or other social media.<br>Requires knowledge of who may be authorised to move money. This may be obtained via phone calls from people claiming to be chasing up payment of an invoice or looking for the contact to send an invoice to. |

## **Appendix II -** Examples of Payment Fraud linked to Cyber-security

**Norwegian Investment Fund – May 2020**

Summary Article
Nor Fund Press Release

*What happened:*

- Fund is currently valued at over a trillion dollars
- Hackers tricked the fund into diverting a $10m loan payment
- They infiltrated communications between the fund and the borrowing organisation and hijacked the information exchange
- They distorted the payment information and the funds were wired to an account in Mexico instead of the correct institution
- The fraud was identified when the scammers initiated a second attempt to do the same

*What could have prevented it:*

In this instance, transfer of documents and payment details via a secure data room may have prevented the hackers from having the opportunity to change the documents. Implementing call back procedures using known contacts to confirm bank account details may also have identified the fraudulent account details.

**Fortelus Capital Management – Dec 2013**

Summary Article

*What happened:*

- CFO received a phone call on a Friday evening purporting to be from Coutts bank about fraudulent activity on the fund's account

- The CFO reluctantly agreed to use the bank's smart card security system to generate codes to give to the caller who would then cancel 15 suspicious transactions
- On Monday it was discovered that $1.5m was missing from the account and Coutts had no record of the Friday phone call
- The CFO was fired and was sued by the Fund for a breach in his duty to protect the fund's assets

*What could have prevented it:*

In this instance the technology and processes were there (payments required codes generated from a smart card security system), it was the person that was the weak link in the chain. Detailed and regular cyber-security awareness training could have prevented this. Understanding that phone calls with a sense of urgency should raise suspicion and that if being asked to do something you are reluctant to do the best option is to phone the other party back on a known number or one sourced from their company website.

**Invoice Fraud**

Given the value of individual transactions, these may not necessarily be publicised. This article has examples from other industries:

Summary Article

*What happened:*

- Kia Motors – Employee set up a fake company and invoiced Kia for over $10m before being caught
- Detroit Metro Airport – Paid a fake invoice for $1.5m for a service that had not been completed
- US Department of Defense – Paid invoices that had deliberately inflated shipping charges that totalled over $20.5m before two sisters were caught
- Google & Facebook – Scammer posed as an employee of a computer company and emailed fake invoices to both firms. He was paid $120m over two years before he was caught

*What could have prevented it:*

The above instances may have been caught through controls such as multiple approvals on payments, approval by a person that understood the services being provided to the firms (or funds) and comparison of invoice costs to a budget of expected expenses.

## **Appendix III -** Electronic Payment System – Illustration of Payment Controls

| Activity | Control Process | Observations |
|---|---|---|
| Bank Account Opening and Power to Bind | The ability to control directions on the bank account should not be given to a sole signatory.<br>Accounts should be set up to require at least two signatories for cash movements and potentially more for large transactions.<br>Accounts that should only transfer cash within the fund structure should be mandated to do so and require resolutions for out of the ordinary transactions. | If the bank being used mandates single signatories, this could make it more vulnerable to cyber-fraud.<br>When additional layers of authorisation are in place, then more work is required to fraudulently imitate these.<br>This will act as an additional red flag point for unusual transactions. |
| Establishment of a new payee (both vendors and investors) | Formal Vendor Approval Process. | Process should involve multiple sign offs either by differing teams or senior individuals to verify payments to this vendor are expected.<br>Payments should not be permitted, unless the vendor has been approved. |
| | Call back is completed to vendor or investor to confirm bank details are correct. | The call back should never be completed using the phone number provided on the invoice or request to change redemption bank details. Either a known number or one sourced from the company website should be used. |
| | Operations team/Fund administrator inputs payment details into the portal. | This can be initiated from either side providing there are strong approval controls in place. |
| | Dual electronic approval from the manager. One approval should be a Senior Operational manager (e.g. Head of Operations, COO etc.) | The preference here is for an operational senior manager to approve, as opposed to a CEO or CIO. The rationale being that this person will be closer to the fund's accounts and will have more knowledge of the types of payments the fund typically makes. |
| | Electronic approval from a senior member of the Fund administrator different to the individual who input the details. (Dual approval if payment details were input by the manager). | This control ensures that two parties (the administrator and the manager) have verified the details. The more people that have looked at the details, the more opportunities to spot errors and/or fraudulent activity. |
| Internal transfers that remain within the Fund structure (e.g. movements | Payment details should be input by a member of the manager's operations team. | Given the cash will not be leaving the Fund (i.e. it remains in accounts in the Fund's name), these transfers do not necessarily need to be initiated by the fund administrator. There may be a preference for consistency with the same process for both internal and external payments. |

| | | |
|---|---|---|
| between PB accounts) | Dual electronic approval should be completed by the manager. Smaller amounts may require a single approval and larger amounts should involve a senior manager. | In this instance, it may be appropriate for the senior manager to be on the investment team as the movements may be trade related. A hierarchy of a approvers relevant to the cash movement size should be documented in a formal cash control policy or authorised signatory lists. |
| External Transfers leaving the fund structure – non-capital activity related | Invoice provided to administrator via electronic means (e.g. through portal or secure data room). | Delivery via a non-email method is preferred. If this is not possible, see additional controls in Example 2. |
| | Administrator verifies payment details to the details stored within the system. | If payment details do not match this should raise a red flag. The verification steps to input new payment details above should be repeated prior to the payment being made.<br>Call backs should be in place to vendors to confirm payment details. Where the volume of payments makes this impractical, a reasonable value threshold should be set and payment above the specified amount should require a call back.<br>Where the invoice is for a reimbursement to the Investment Manager, the administrator must ensure to receive the original invoice, reconcile against Fund budgets and validate any allocations across multiple funds are correct. |
| | Administrator inputs payment into the portal | The process may originate with the operations team at the manager inputting the payment and uploading the evidence into the portal. As long as dual electronic approval, at both the manager and administrator, remains in place this is still a strong control. |
| | Dual electronic approval from the manager with one approval being from a senior operational manager (e.g. Head of Operations, COO etc.) | As above, an operational senior manager will have more insight into invoices that the fund typically pays and vendors that it uses. |
| | Dual electronic approval at the administrator to release the payment. | To prevent internal fraud or misappropriation of assets, the administrator should be the only party that is authorised to physically make payments to external parties. |
| Capital Activity Movements (i.e. Subscriptions and Redemptions) | If applicable, the administrator verifies bank details provided on the redemption request to stored bank details. | This will be in addition to standard AML checks required prior to releasing redemption proceeds. If bank details do not match the process described above for inputting, new bank details should be followed.<br>For movement of subscription amounts from the Subs/Reds account to the trading accounts, the administrator should be in full control of this cash movement (following a dual authorization process) in order to ensure any regulatory requirements (e.g. source of funds checks) have been completed prior to the capital being made available for trading. |

| | | |
|---|---|---|
| | Administrator provides the investment manager with details of all capital activity and inputs payments into portal | The administrator is the party in control of investors transactions and should therefore initiate this process.<br>Best practice would be for this to be provided via a secure web-portal. If the document is to be provided via email, then the controls mentioned above should be followed. |
| | Dual electronic authorization at the manager including a Senior manager. | For mutual funds, UCITs funds etc. it may not be practical for the manager to approve all payments. An alternative to this is a bulk approval of upcoming redemptions to the administrator (again delivery of this via a secure web-portal or data room would be preferred). The manager would then move the corresponding amount from the trading accounts to the PB accounts. |
| | Dual electronic authorization at the administrator to release the payment. | The administrator should be the only party authorised to physically move money to external parties. |
| Detective Controls - Reconciliations | Daily cash reconciliations completed by the administrator ensuring all cash movements can be validated. | Capital activity and invoice payments should be booked into the accounting system when payments are instructed. Erroneous cash payments that cannot be tied back to these can then be identified. |
| | Daily cash reconciliations completed by the manager (or the manager's outsourced middle/back office provider) | These reconciliations should be independent of the administrator who was instructed the physical release of the payment. This will then act as a second validation that cash movements out of the account where expected/valid. |
| | Reconciliation of invoices paid to the Fund's pre-agreed expense budget. These should take place at a minimum in line with the Fund's valuation frequency. | A budget of expected fund expenses should be agreed between the manager and the administrator on an annual basis. Reviewing invoices against these budgets will highlight if the expense is unexpected or if the amount paid is larger than was anticipated. |

## **Appendix IV -** Non-Electronic Payments – Illustration of Payment Controls

For any document that is sent via email relating to cash movements e.g. invoices, payment instructions or authorisations, strict cyber-security protocols should be followed.

These controls would include:

- Approval should be via signatures on a scanned payment instruction that can be verified back to an Authorised Signatory List that has been approved by the Fund Board, where applicable, or other formal governing body for the Fund or firm
- Approval via email should not be accepted by the administrator as this is open to cyber-attacks.
- The scanned instruction sent to the administrator should ideally be transferred via the administrator's secure web-portal (if it allows uploads), secure data room that has user-controlled access or other secure electronic document transfer process

- In the event these need to be sent via email the document should be password protected with a password agreed in advance and provided to the administrator via a non-email format (i.e. via a telephone call). This would alert the administrator to the possibility of a fake invoice should a payment instruction be received without this password in place
- Wherever possible, emails should be sent to or include group distribution lists so a greater number of people are aware of a cash movement and can raise any issues

| Activity | Control Process | Observations |
|---|---|---|
| Establishment of a new payee (both vendors and investors) | Call back is completed to vendor or investor to confirm bank details are correct. | The call back should never be completed using the phone number provided on the invoice or request to change redemption bank details. Either a known number or one sourced from the company website should be used. |
| | Operations team/Fund administrator inputs payment details into banking system or other golden source document. | This can be initiated from either side providing there are strong approval controls in place.<br>Where using a golden source document, as opposed to a banking system the document should be password protected with only authorised signatories having access to the password. The document should maintain an audit trail of changes and approvers.<br>Storing agreed payment details outside of a user-controlled system is a weak cash control and open to abuse. This should be avoided where possible. |
| | Dual approval from the manager. One approval should be a Senior Operational manager (e.g. Head of Operations, COO etc.) | Approval should be via signatures on a scanned payment instruction that can be verified back to an Authorised Signatory List that has been approved by the Fund Board.<br>The email controls noted above should be followed.<br>The preference here is for an operational senior manager to approve, as opposed to a CEO or CIO. The rationale being that this person will be closer to the fund's accounts and will have more knowledge of the types of payments the fund typically makes. |
| | Approval from a senior member of the Fund administrator different to the individual who input the details. (Dual approval if payment details were input by the manager). | This control ensures that two parties (the administrator and the manager) have verified the details. The more people that have looked at the details, the more opportunities to spot errors and/or fraudulent activity. |
| Internal transfers that remain within the Fund structure (e.g. movements | Payment details should be input by a member of the manager's operations team. | Given the cash will not be leaving the Fund (i.e. it remains in accounts in the Fund's name), these transfers do not necessarily need to be initiated by the fund administrator. There may be a preference for consistency with the same process for both internal and external payments. |

| | | |
|---|---|---|
| between PB accounts) | Dual approval should be completed by the manager. Smaller amounts may require a single approval and larger amounts should involve a senior manager. | Most counterparties will provide a payment portal for these types of transactions which should be used as best practice. In the event this is not possible, the email controls noted above should be followed.<br>In this instance, it may be appropriate for the senior manager to be on the investment team as the movements may be trade related. A hierarchy of approvers relevant to the cash movement size should be documented in a formal cash control policy or authorised signatory lists. |
| External Transfers leaving the fund structure – non-capital activity related | Invoice provided to administrator via electronic means (e.g. through portal or secure data room) | Wherever possible, invoices should be sent to the administrator via a non-email format. For example, an administrator secure web-portal (if it allows uploads), via a secure data room with user-controlled access or other secure electronic document transfer. This would make invoices received via email an unusual occurrence that needed further scrutiny.<br>Any invoices delivered from the manager to the administrator should be signed by someone on the manager's authorised signatory list. This confirms to the administrator that the manager has validated the invoice.<br>If invoices are to be sent via email, the email controls noted above should be followed. |
| | Administrator verifies payment details to the details stored within the system. | If payment details do not match, this should raise a red flag. The verification steps to input new payment details above should be repeated prior to the payment being made. |
| | Dual approval from the manager with one approval being from a senior operational manager (e.g. Head of Operations, COO etc.) | Where approval is being given via non- electronic means, the approval should be a scanned document with signatures that can be verified to the authorised signatory list. Where these scanned instructions are being sent via email, the email controls noted above should be followed.<br>As above, an operational senior manager will have more insight into invoices that the fund typically pays and vendors that it uses. |
| | Dual approval at the administrator to release the payment. | To prevent internal fraud or misappropriation of assets, the administrator should be the only party that is authorised to physically make payments to external parties. |
| Capital Activity Movements (i.e. Subscriptions and Redemptions) | Administrator provides the investment manager with details of all capital activity. | Best practice would be for this to be provided via a secure web-portal. If the document is to be provided via email, then the email controls noted above should be followed. |

| | | |
|---|---|---|
| | If applicable, the administrator verifies bank details provided on the redemption request to stored bank details. | This will be in addition to standard AML checks required prior to releasing redemption proceeds. If bank details do not match the process described above for inputting, new bank details should be followed.<br>For movement of subscription amounts from the Subs/Reds account to the trading accounts, the administrator should be in full control of this cash movement (following a dual authorization process) in order to ensure any regulatory requirements (e.g. source of funds checks) have been completed prior to the capital being made available for trading. |
| | Dual authorization at the manager including a Senior manager. | For mutual funds, UCITs funds etc. it may not be practical for the manager to approve all payments. An alternative to this is a bulk approval of upcoming redemptions to the administrator (again delivery of this via a secure web-portal or data room would be preferred or email controls noted above should be followed). The manager would then move the corresponding amount from the trading accounts to the PB accounts. |
| | Dual authorization at the administrator to release the payment. | The administrator should be the only party authorised to physically move money to external parties. |
| Detective Controls - Reconciliations | Daily cash reconciliations completed by the administrator ensuring all cash movements can be validated. | Capital activity and invoice payments should be booked into the accounting system when payments are instructed. Erroneous cash payments that cannot be tied back to these can then be identified. |
| | Daily cash reconciliations completed by the manager (or the manager's outsourced middle/back office provider) | These reconciliations should be independent of the administrator who was instructed the physical release of the payment. This will then act as a second validation that cash movements out of the account where expected/valid. |
| | Reconciliation of invoices paid to the Fund's pre-agreed expense budget. These should take place at a minimum in line with the Fund's valuation frequency. | A budget of expected fund expenses should be agreed between the manager and the administrator on an annual basis. Reviewing invoices against these budgets will highlight if the expense is unexpected or if the amount paid is larger than was anticipated. |

## Appendix V

Investor Payments (Capital Calls/Subs/Reds) - Illustration of Payment Controls

| Activity | Control Process | Observations |
|---|---|---|
| Closed Ended Funds – Capital Call Notices | Agree with administrator of fund (or other party in the event there is no administrator) how capital calls will be delivered, expected frequency and the format of the capital call notice. | Where possible, any capital call notices should be received via a secure web-portal that requires the investor to log in to retrieve the capital call notice. Most fund administrators will provide this option and investors should push managers to utilise this service from their administrator. If to be delivered via email, discuss with the administrator whether documents can be password protected with a pre-agreed password. Receipt of capital call notices via an unprotected emailed attachment is a weak control that is open to cyber-attacks.<br>Discuss with the manager how often they anticipate sending capital call notices – there may be regular times for calls for fee payments. Understand whether there will be any communication from the manager in advance of receiving the capital call notice.<br>As part of the due diligence process, obtain an example template of the format that the capital call notice will take. This can then be used to compare any received capital call notices to as an additional check |
| | Operations team sets up payment instruction within payment system. This would then have dual approval including a senior operations person. | Payment details should be obtained from the fund's documents and any accounts should be in the name of the Fund.<br>In the event the investor is notified of a change in bank details (which should be a rare occurrence), the procedures for verifying payment details noted in the cash movements section above should be followed. |
| | Capital call notice should be verified by operations including that it was expected, received in the correct format and contains the same bank account details that have previously been set up. | If method of delivery, format of document, bank account details are not what was expected or no advance notice had been given of this capital call, the operations team should complete a call back to the administrator (using a known number or one from the company website) to verify the capital call is valid. |
| | Payment is input into payment portal by a member of the operations team. Dual approval from Senior operations person and Senior investment team person. | In the event a payment portal is not being used and payment instructions are being emailed to a custodian or other third party to make the payments, then all controls (including email controls) detailed in the external payments sections above should be followed.<br>The combination of operations and investment team approval helps to validate the payment from two perspectives. Firstly, that the amounts and bank details provided are correct (operations) and secondly, that the capital call is in line with the investment team's understanding of their investment. |
| Open Ended Fund – Subscription Payments | These payments should follow all the controls detailed above for external payments whether being instructed via a payment portal or via email instructions. | |

## **Appendix VI –** Workstream Members

The SBAI would like to thank the following members of the Governance Working Group for their participation in the production of this Toolbox Memo.

**Elena Manola-Bonthond**
CIO – CERN Pension Fund

**Roman Goosens**
Economist – CERN Pension Fund

**Betty Martin**
Director of Investment Services – Employees Retirement System of Texas

**John Richardson**
Chief Operating Officer and General Counsel – Ionic Capital Management

**Ritesh Patel**
Due Diligence & Advisory – Ontario Teachers' Pension Plan

**Alex Baker**
CTO – Orchard Global Asset Management

**Nathalie Bouchard**
Senior Director, Operational Due Diligence and Advisory – Public Sector Pension Investment Board (PSP Investments)

**Kathy Farrel**l
Director, Operational Due Diligence and Advisory – Public Sector Pension Investment Board (PSP Investments)

**Nicholas Miller**
Virtual CISO – Aedile Consulting