

## Executive Summary

Objectives of Forensics [S.1](#)

Pre-Engagement Steps [S.2](#)

Document Checklist [S.3](#)

*“The Choice for  
Global Professional  
Services”*

Proper handling of  
evidence is every team  
member’s responsibility.

## Checklist & Guidelines in Preparation for Forensics.

### *ACCUMERIC—Forensic & Transaction Support*

When suspicion of malicious or illegal acts is present, there are several time-critical steps that both the complainant and the forensic professionals should do. Below is a general guide to help increase the chances of success as well as to mitigate loss and the risk of contaminating evidence.

#### **Type A: Broad Step-Plan**

The objective of Forensic & Investigative Services (“FIS”) in cases of suspicion is to:

- (i) gather background and fresh intelligence from both the field and management
- (ii) identify who is part of the trusted network and remain invisible, when applicable
- (iii) predetermine a date or an objective trigger event when to contact the authorities
- (iv) isolate & monitor existing security gap
- (v) search for connectors and other lapse in control
- (vi) identify the immediate incident and suspected perpetrators
- (vii) pull employment records and conduct background search, when applicable

- (iv) investigate possible co-conspirators within the organization
- (v) expand the scope, when applicable
- (vi) formulate a plan to collapse the perimeter within an appropriate pace
- (vii) quantify the loss for insurance and litigation purposes.

Type A is an over-simplified chronology of the events, but in practice, the actual procedures, chain of tests and examination will be based on facts and circumstances. It can involve a team of technology consultants sifting through networks, hard-drives, external sources, websites, mobile phones, voice mails, video surveillance and access systems. It can also involve private investigators conducting outside searches including both public and private data bases. FIS will work with clients in developing and exercising the appropriate action plan given the situation at hand.



## What steps to take?

### General Checklist to help FIS

Cooperation is vital between the organization and FIG to mitigate further loss and to assist the investigation effectively and with purpose. The checklist below may help provide guidance during an ongoing examination:

- (i) selectively inform the audit and/or board committee [Trusted Network]
- (ii) if the company's general counsel is unreliable, work with the Trusted Network in possibly engaging an outside attorney specializing in such delicate matters
- (iii) remind or reinstate company policy of document retention, subject to routine quality control checks
- (iv) begin archiving both hard and digital data ensuring the data remains un-tampered with
- (v) physical security of premises and assets of the company should be revisited
- (vi) circle back to isolate the source of the risk
- (vii) work with the Trusted Network as to when to contact the insurance company
- (viii) work with the Trusted Network as to when to contact the proper authorities and regulators
- (ix) work with the Trusted Network as to when to begin securing outside information about the perpetrators

with the intention of furthering the investigation and identifying other risks within the organization (e.g. public records, reconstructing net-worth statements, bank records, travel patterns, etc.)

### Document Handling as Part of an FIS Engagement

The two prior sections points out the steps taken by both FIS and the organization to coordinate efforts in the most efficient manner possible. The following section is a checklist of document handling procedures that should be considered during an ongoing investigation. It is worth noting that adequate security, a proper evidence index-system and offsite working copies are made available to the forensic, litigation and special committee within the trusted network should be considered as well as establishing clear policy regarding improper dissemination of the information at hand.

- (i) full report detailing the complaint/allegation
- (ii) Approved schedule, work-plan, pre-determined milestones and triggers
- (iii) original interview questionnaire, interview log, minutes and transcripts
- (iv) electronic and hardcopy documents, internal/external communications and evidence
- (v) relevant photographs and video tapes
- (vi) all materials should be handled signed concurrently by one agent of the Trusted Network and another from forensic & litigation team.

### Contact Information

Accumeric  
80 Broad Street, 5th Fl  
New York, NY 10004  
(877) ACC—8304

Uncovering fraud, malicious or illegal acts, or corporate sabotage can be an intense situation and should be handled with a great deal of care. The preceding materials are meant to inform as well as to provide you with the first steps in taking action.

Accumeric.com

