Fraudsters at the Gate: How Corporate Leaders Confront and Defeat Institutional Fraud—Part 2

Martin S. Kenney[*]
Managing Partner, Martin Kenney & Co, Solicitors, BVI

Alex D. Moglia[**]
President, Moglia Advisors, Financial Advisors, Chicago

Alexander Stein, PhD[***]
Founder, Dolus Advisors, New York

Banks; Companies; Corruption; Fraud; Money laundering; Risk management

Abstract

This is the second section of a two-part article addressing challenges that serious fraud poses for corporate leaders, stakeholders and victims. Here, we examine common executive reactions to fraud and offer tools for senior leaders to more effectively recognise and respond to danger signs. We also discuss the collateral social and economic impact of large-scale institutional frauds and conclude with practical recommendations for mitigating white-collar malfeasance risks.

This is the second section of a two-part article addressing challenges posed by serious fraud for corporate stakeholders and victims beyond economic, reputational and other obvious losses. In the first part, published in the previous edition of JIBLR,[1] we discussed key issues, duties and responsibilities senior corporate leaders confront when their institution has been defrauded. We also covered the impact of compliance, management of fraud and money laundering risks and building effective anti-money laundering (AML) plans based on ethics and regulatory compliance.

In this second part, we address tools, danger signs, reactions to fraud—including some institutional leaders' reflexive response for self-preservation over safe-guarding their organisation's best interests—and the common pitfalls of racing to the scene of an apparent fraud. We also discuss issues relating to the negative collateral public impact of large-scale frauds: the harm to additional classes of victims besides investors, employees or vendors and the consequent damage to the social and economic fabric. We conclude by delineating recommendations for senior management that include pursuit of the greater good, rather than hiding behind corporate aprons to avoid what's often perceived as the greater bad.

Tools

Tools are implements for carrying out particular tasks or functions. Corporations regularly deploy batteries of tools in counter-fraud, anti-corruption, cybersecurity and general malfeasance threat mitigation and defence work. Some are complicated, others are not; some are expensive, others are less so; some require great effort, others not as much. Many of the tools commonly used in companies, banks and financial institutions to combat white-collar threat risks are the equivalent of simple machines: mechanisms using a mechanical advantage to multiply force. Examples of actual simple machines include the lever, the pulley and the wheel. In corporate compliance and risk mitigation, analogous instruments include checklists, risk and integrity audits, employee training, monitoring programs (both human and software), operational risk identification and management control systems, and statutory and regulatory cross-checking, among many others.

While all of these instruments have functional values of varying degrees and in varying scenarios, by design, none can exceed its elemental limitations. As every competent worker knows, there is a right tool for every job. Knowing which is both a science and an art. Our contention here is that the majority of tools typically used to detect, understand, identify, mitigate and defend against fraud, corruption, cybercrime and many other malicious attacks, are frequently incorrect, insufficient or both. In addition, we take the position that operations designed to effectuate mitigation, prevention and recovery must be predicated on accurate and sophisticated analyses of the problems they are intended to resolve.

A common pitfall in many fraud, corruption and cybercrime risk mitigation and defence systems is that they are designed, by and large, only to notice the noticeable. More often than not, important datasets will not register as potentially amiss until there is something potentially amiss to note. This is the equivalent of oceanographers only observing the water's surface and failing to correlate seismic activity with the increased likelihood of a tsunami forming at great depths. The constitutive elements of what could be discernible or interpretable as an early indicator (or warning) of an impending event can be exceedingly difficult to spot or put into meaningful context. Achieving this level of

[*] Contact at: *mkenney@mksolicitors.com*.
[**] Contact at: *amoglia@mogliaadvisors.com*.
[***] Contact at: *alexanderstein@dolusadvisors.com*.
[1] Martin S. Kenney, Alex D. Moglia and Alexander Stein, "Fraudsters at the Gate: How Corporate Leaders Confront and Defeat Institutional Fraud—Part 1" (2016) 31 J.I.B.L.R. 571.

predictive threat awareness requires specialised intelligence gathering and analysis with which to triangulate significance, minimise false-positives and cull static and noise from important but fragmentary or cryptic material.

Perfect blueprints do not guarantee a perfect structure, particularly in situations where the human element is central. Fraud and other forms of white-collar malfeasance induce or seduce victims to unwittingly become deprived of dominion over their (or a company's) money or other valuable assets through deceit, artifice, sharp practice, or breach of confidence. Institutional risk and compliance programs and procedures need to protect critical functionalities and vulnerabilities, and be in conformity with all necessary requirements and best practices. However, such systems must also be designed to account for the universe of unpredictable complex human elements which cannot be captured by procedure alone.

With this in mind, our view of the additional tools needed to combat corruption and fraud include creativity and innovation, together with a broader appreciation for the constituents and drivers of malicious action and the institutional dynamics which can cultivate or delimit malicious acts.

A blueprint for directly integrating culture and ethics into core commercial services and risk management practices must include sophisticated assessment tools and protocols capable of scanning, analysing and responding to the following:

- mens rea, intentional and unconscious actions;
- the appearance of compliant or ethical behaviour within an organisation, which may be masking a different reality;
- the shortcomings of standard screening devices (which are challenged to pre-test for integrity and honesty as native characteristics); and
- misrepresentation, exaggeration, enhancement, minimisation, falsification, avoidance and other human tendencies to distort the true picture.

Standardised testing and questionnaires, popular in many companies, can serve useful functions, but narrative assessments coupled with mediated (or moderated) interviews—though more costly and time-consuming—invariably yield more meaningful information. Even more important than the specific instruments used are the methodology of deployment and interpretation of data harvested. Subsequent steps involve how the data is synthesised, analysed and interpreted to account for a range of influential dynamics, elements, collection methods and limitations, and various other hard and soft variable factors which may not be captured, or the implications of which might be overlooked in a simple or one-pass operation.

Reviews, assessments and evaluations are often dreaded moments in many organisations. Recognising the opportunities they present, however, not just their limitations and challenges, is of primary importance. From a threat mitigation standpoint, these exercises are a unique inflection point for involving employees as stakeholders in culture-building and internal perimeter fortification. If structured and deployed well, evaluations can achieve more than just returning binary responses about performance/competency metrics or indicating talent development/retention pathways. They can yield rich veins of data about many facets of institutional life which have a direct and indirect bearing on internal security and culture, not just on skills and productivity.

We therefore recommend institutions reframe conventional understandings and uses of self-reporting. Rather than a flawed but unavoidable necessity and source for concern, they are more productively considered part of a dynamic field of ingredients which will inform senior leaders about their institution and its people.

Danger signs

In Pt 1 of this article, we discussed the pressures on international banks' top management to grow their institutions' revenues and profits. These pressures often lead to actions being taken or decisions made without due regard to potential pitfalls or increased likelihood for abuse. The unbridled drive for profit often leads to shortcuts being taken with potentially catastrophic consequences. Consider the relationship between Royal Bank of Canada (RBC) and Gilberto Miranda Batista. In August 2015, *The Wall Street Journal* published an article entitled "Inside Royal Bank of Canada's Latin Misadventure"[2] about Royal Bank of Canada's aggressive drive to attract high net worth customers in Latin America. The article focused on the fall-out from a now-closed Miami office of the Bank which had reeled in big fish Mr Miranda, a former Brazilian senator with a US $500 million fortune. RBC's compliance department tried to put a damper on the celebratory mood, even recommending that the accounts be closed. As early as 2007, RBC compliance officers raised concerns that the accounts might attract scrutiny from global regulators over potential money laundering but the Miami-based RBC banker who had introduced Mr Batista to RBC successfully argued against such closures. When Brazilian prosecutors charged Batista with corruption in 2012, it would have seemed a good time to shut those accounts. However, it was not until Batista was eventually indicted and the Office of the Comptroller of the Currency deemed RBC's AML controls unsatisfactory that action was finally taken. Ultimately, the bank closed the Miami office and the banker in charge of the accounts faded into the

[2] Alistair Macdonald and Rita Trichur, "Inside Royal Bank of Canada's Latin Misadventure" (2015), *The Wall Street Journal* available at: *http://www.wsj.com/articles/inside-royal-bank-of-canadas-latin-misadventure-1438828641* [Accessed 28 October 2016].

background. Batista was deemed a "politically exposed" foreign person and the bank severed its relationship with him.

Such incidences of gross failure to identify or appreciate risks—or worse, turning a blind eye—do nothing to foster confidence in the banking system. Warning signals must be acted upon, not just identified. Staff must be taught to recognise and report certain signs or "red flags" so that timely action can be taken. Ultimately, management bear the responsibility for ensuring that staff are adequately trained to appreciate and understand risks of varying levels or types, and then to report instances of conduct arousing suspicion. Management are also responsible for investigating and, as determined, acting decisively.

In the US, the Securities and Exchange Commission (SEC) and the Office of the Comptroller of the Currency look at banks' financial statistics and managements' behavioural patterns. Anti-fraud corporate and regulatory teams look for red flags manifested in banks' relationships with customers, vendors and government officials, as well as in merger and acquisition due diligence related to contemplated transactions. They have developed a comprehensive list of danger signs or red flags. While we do not propose to reiterate that red flags list, Rob Biskup and Bill Pollard, both of Deloitte, describe some red flags in a 2015 article in *CFO Magazine* entitled "Deep Due Diligence Needed in Emerging Markets Deals",[3] among them:

- cash payments without supporting documentation;
- consulting or processing fees that may be disguised bribes;
- incomplete documentation and/or explanations regarding specific transactions;
- transactions that are questionable or may expose banks to civil and/or criminal prosecution;
- antitrust laws that may make information inaccessible;
- separation of tax and accounting departments that are kept isolated from each other;
- multiplicity of transactions/loans among related entities;
- financial statements that do not make sense;
- use of a bevy of parties for what would otherwise be fairly straightforward transactions;
- purchases or sales of assets or entities at prices that seem unusually high or unusually low; and
- high turnover of personnel, consultants, or auditors; alternatively, auditors that do not seem to be geographically linked to the banks and/or customers and vendors.

This is only a sampling; a roster of every potential danger sign would be nearly endless. Each banking institution must develop its own list of red flags tailored to its areas of activity, geographic location and client base. Other factors that can influence the red flag list include whether correspondent banks are commonly used and where they are located, as well as known patterns of fraud in an area of business or country and the services offered there.

The US Federal Financial Institutions Examination Council's AML manual and The Financial Action Task Force (FATF) have also identified a number of indicators of trade-based money laundering activities. These high-probability AML red flags predominantly derive from observations logged in Suspicious Activity Reports (SARs) in the US. Red flags are not proof of illegal activity. They are indicators that money laundering may be occurring—for instance, unexpected or unusual transaction activity, service or goods traded, value or geographical location—and should prompt further investigation. As noted above, every institution must custom-tailor its own list of warning signs based on variable institution-specific criteria. However, the combined indicators listed by the US Federal Financial Institutions Examination Council and the FATF form a comprehensive list of red flags for trade-based money laundering which can be applied to both the trade and financial sectors. These are:

- inability of a bank customer to produce trade documentation to back up a requested bank transaction;
- significant discrepancies appear between the description of the commodity on the bill of lading and the invoice;
- significant discrepancies appear between the description of the goods on the bill of lading or invoice and the actual goods transported;
- significant discrepancies appear between the value of the commodity reported on the invoice and the commodity's fair market value;
- shipment locations or description of goods that are inconsistent with the letter of credit;
- documentation showing a higher or lower value or cost of merchandise than that which was declared by a shipper or paid by an importer;
- a transaction that involves the use of amended or extended letters of credit that are amended significantly without reasonable justification or that include changes to the beneficiary or location of payment;
- a third party paying for the goods;

[3] Available at: *http://ww2.cfo.com/ma/2015/07/deep-due-diligence-needed-emerging-markets-deals/* [Accessed 28 October 2016].

- a consignment that is inconsistent with the business (e.g. a steel company that starts dealing in paper products, or an information technology company that suddenly starts dealing in bulk pharmaceuticals);
- customers conducting business in high-risk jurisdictions. Although not specifically identified by the US Federal Financial Institutions Examination Council, Free Trade Zones (FTZs) may be added to the list of high-risk jurisdictions given that there is an argument that FTZs exacerbate the risk;
- customers shipping items through high-risk jurisdictions, including transit through non-co-operative countries;
- the commodity is transhipped through one or more jurisdictions for no apparent economic reason;
- customers involved in potentially high-risk activities, including those subject to export/import restrictions such as equipment for military or police organisations of foreign governments, weapons, ammunition, chemical mixtures, classified defence articles, sensitive technical data, nuclear materials, precious gems or certain natural resources such as metals, ore and crude oil;
- obvious over- or under-pricing of goods and services;
- obvious misrepresentation of quantity or type of goods imported or exported;
- a transaction structure that appears unnecessarily complex so that it appears designed to obscure the transaction's true nature;
- a shipment that does not make economic sense (e.g. the use of a large container to transport a small amount of relatively low-value merchandise);
- consignment size appears inconsistent with the scale of the exporter or importer's regular business activities;
- the type of commodity being transported appears inconsistent with the exporter or importer's usual business activities;
- the method of payment appears inconsistent with the risk characteristics of the transaction, for example, the use of an advance payment for a shipment from a new supplier in a high-risk country;
- a transaction that involves receipt of cash or payment of proceeds (or other payments) from third-party entities that have no apparent connection with the transaction or which involve front or shell companies; and
- a transaction that involves commodities designated as high risk for money laundering activities, such as goods that present valuation problems or high value, high turnover consumer goods.

While helpful as a standalone guide, lists like this must be properly implemented to be effective. Employees must be trained how to observe and monitor so that potential red flags do not go unnoticed, significance in context is appreciated and sequenced responses are triggered. However, recognising danger signs must not be confined to "tick the box" or blind categorisation. Often, an over-focus on defined categories or "signs" leads to scenarios where people miss the wood for the trees. Astute peripheral vision, critical thinking and sound judgement must be instilled as integral aspects of programs designed to detect potential money laundering or other fraudulent activity.

Enhanced due diligence is an essential component of the tool kit when forging new business relationships, yet it generally remains under-established and often inadequately utilised. Experience shows that companies take significant and otherwise avoidable risks when they transact without first performing detailed research to verify all relevant bona fides. One area where banks are particularly vulnerable is client referral. Consider situations where a third party "vouches" for a client or where a correspondent bank is involved. Many institutions take the view that referrals of those sorts do not always necessitate thorough or detailed due diligence. This would, however, be an undue risk. When prospective clients are referred by a third-party entity, banks must ensure that the due diligence documentation provided by that third party relates directly to the prospective client and all relevant information must be verified and cross-checked. The usefulness of categorised "red flags" or "danger signs" is underscored when appropriately linked to the broader due diligence apparatus. Together, these mechanisms enable institutions to mitigate risks or avoid other problems down the line by methodically screening vendors, customers and transactions.

Reactions to fraud

Notwithstanding careful due diligence, assiduous monitoring of typical danger signs and other detect–defend programs, fraud is, unfortunately, a nearly unavoidable inevitability for many organisations. It occurs with alarming frequency despite efforts to guard against it. It is therefore vital that banks have established protocols in place to handle the fall-out when fraud strikes.

Race to the scene of the crime

When it becomes apparent that a fraud has been perpetrated, the first steps taken upon discovery can make the difference between the success or failure of the ensuing investigation, remediation, recovery and

reputation–rehabilitation efforts.[4] When we speak of racing to the scene of the crime, we are not referring to a high-speed chase with sirens blazing, "do not cross" tape or any other typical crime-scene props. Indeed, in fraud, the responses we recommend are quite the contrary. Often, the perpetrator will not be aware that the discovery has been made. More often than not, the ostensible scene-of-the-crime is unknown and may not even be a physical scene at all; in banking, invariably, there is none. The scene of the crime refers to the milieu—the general environment—in which the event occurred. However, just as in common physical crimes, the scene of the crime usually holds important keys.

One of the most important aspects of evidence collection and preservation is protecting the crime scene. In fraud cases, this invariably involves maintaining utmost secrecy regarding what we know while determining what we do not. The integrity of all evidence, physical, digital and otherwise, must be maintained. The race to the scene must involve experienced digital evidence gatherers to secure all materials before the perpetrator has an opportunity to delete his or her tracks (assuming this has not already been done). Some digital evidence requires special collection, packaging and transportation techniques. Given the speed and ease with which digital information can be altered, computer forensic professionals play an integral early role.

Potential digital evidence in online or economic fraud investigations includes:

- computers;
- removable media;
- mobile communication devices;
- external data storage devices;
- online auction sites and account data;
- databases;
- PDAs, address books and contact lists;
- printed email, notes and letters;
- calendars or journals;
- financial asset records;
- accounting or recordkeeping software;
- printed photographs and image files;
- records or notes of chat sessions;
- information regarding Internet activity;
- customer credit information;
- online banking information;
- credit card numbers;
- telephone numbers and call logs;
- credit card magnetic strip readers;
- credit card statements or bills; and
- printers, copiers and scanners.

As noted, maintaining integrity of evidence is of paramount importance; many a case is won or lost on the basis of evidence contamination or a break in the chain of control. The notion of cross contamination at the crime scene or in a DNA laboratory is easily understood. Digital evidence can be analogously compromised or contaminated. This must be prevented by those tasked with collection. Prior to analysing digital evidence, an image or work copy of the original storage device is created. When collecting data from a suspect device, the copy must be stored on another form of media to keep the original isolated. "Clean" storage media must be used in order to prevent the introduction of data from another source, or any other type of contamination. Simply erasing data on a media source and replacing it with new evidence is not sufficient, the destination storage unit must be new; if reused, it must be forensically "wiped" prior to use—this removes all known and unknown content from the media.

Former National League Football star, O.J. Simpson was tried on two counts of murder in Los Angeles County Superior Court in a trail commencing in November 1994. He was acquitted following a verdict issued by the jury after only four hours of deliberation on 3 October 1995.[5] The case highlighted the implications of flawed evidence gathering. The highly publicised trial provided a textbook case study in what *not* to do while processing evidence at a crime scene. O.J. Simpson's defense attorney, Johnnie Cochran, referred to the Los Angeles Police Department's scientific investigations division as a "cesspool of contamination" for its sloppy evidence handling.

Gather and understand facts

Fraud cases typically involve complex webs of misrepresentations by many people (whose true identities may not be known for some time) through many companies (or shell companies) and in multiple jurisdictions. Gathering, analysing and understanding the fraudulent scheme and identifying who is involved and where they are located involves tremendous time and effort. While evidence gathering in fraud cases differs from the process used in straightforward cases of theft, the basic principles remain largely the same: follow the most visible trail to and/or from the scene of the crime. Digital or physical footprints or other identifying markers may have been erased but in the majority of cases there will be some clue, hint, or pointer, however minuscule, that can lead the investigator in a particular direction. Of course, in fraud cases, all is probably not what it seems. Sophisticated fraudsters frequently intentionally plant false clues to throw investigators off the real trail. Deliberate analysis, skepticism and experience are critical.

[4] As part of the planning/assessment process, it is imperative that one establish whether or not the investigation is geared to the employee's termination/civil recovery alone or if there is a possibility of escalation to criminal prosecution. If the latter, one must consider engaging with law enforcement as soon as practicable for guidance, as interviewing suspects in the absence of a Caution/Miranda Warning may render evidence obtained by internal investigations inadmissible. In addition, consideration should be given in the US to giving an Upjohn Warning should an interview be conducted by counsel to an employer, where appropriate (available at: *http://www.americanbar.org/content/dam/aba/administrative/labor_law/meetings/2011/ac2011/137.authcheckdam.pdf* [Accessed 28 October 2016]). It must be stressed that there are variances between jurisdictions; therefore there can never be a one-size-fits-all solution.

[5] *People of the State of California v Orenthal James Simpson* available at: *http://law2.umkc.edu/faculty/projects/ftrials/Simpson/Simpsonchron.html* [Accessed 28 October 2016].

Perceptive analysts will be alive to the probability of evidentiary obfuscation and dissembling. However, even the sophisticated methods a fraudster uses to obscure his tracks are themselves pieces of evidence subject to insight-producing analysis. Human factor specialists, whose initial function on the fraud investigation team is analogous to the criminal profilers commonly used in homicide investigations, can develop a provisional understanding of the fraudster's mindset through contextual interpretation of residual psychological fingerprints and soft data signatures imprinted in the scene.

Despite the plethora of new digital evidence gathering techniques at our disposal in this digital era, the primary methods for gathering evidence continue to be traditional witness examinations and document discovery, including electronic documents. New technologies can hamper investigators' ability to gather electronically stored evidence. Many contemporary network security technologies and strategies can actually prevent law enforcement, justice agencies, private investigations firms and prosecutors from executing lawful court orders to access and secure electronic evidence or to thoroughly investigate criminal or terrorist incidents. The recent situation involving Apple and the FBI[6] is a prime example of a face-off between a commercial technology company and law enforcement where each asserted differing positions on, respectively, the right to protect or access electronic information. This case arose following the attacks in San Bernardino, California on 2 December 2015 in which 14 people were murdered and 22 injured. The two shooters were eventually killed by the police and their computer equipment and iPhones were confiscated. The authorities were unable to unlock one of the shooter's iPhones, which was believed to hold information potentially important to the case. Apple refused to create a work-around master key to circumvent security features in the iPhone operating system to enable the FBI to retrieve data from the deceased suspect's iPhone. Ultimately, the FBI announced it had accessed the information without Apple's help (by paying a Black Hat to hack the device). It is a case study in the technical challenges, privacy concerns, and colliding legal and commercial interests in accessing encrypted information in the context of a criminal investigation.

Electronic evidence can be categorised as: "real data", which includes the specific content of an email, text message or voice call; or "meta data", which is information about information, for example, date and time stamp and server location of an email, transaction, geo-tagged photo or sale/transaction data. Often, the meta data can be particularly useful in advancing a case. As with nearly all ostensible clues in fraud cases, intentional deception is to be anticipated. Experienced fraudsters typically will not record their intentions or actions in written formats such as emails or texts, or they will deliberately falsify this data trail. Nonetheless, irrespective of the content of any e-data, an IP session address or IP destination address can lead to a suspect's location or allow an investigator to establish or trace a pattern of activity. Identifying and interpreting all forms of data is critical to building and advancing the case.

Once it has been confirmed that assets have been misappropriated, the next priority is to verify that assets exist in an attachable form. Gathering such evidence involves identifying who is responsible and who may be liable, including possible facilitators such as other banks, advisors or simple recipients. The investigation will need to locate and define the manner of holding of concealed assets believed attributable to principal targets, including real property, investments, links to businesses, financial holdings and other sources of income. The investigation of principal targets may include:

- surveillance;
- covert retrieval of evidence and records;
- pretext contacts; and
- other investigative activities to ascertain means of lifestyle funding.

Base-line, comprehensive background investigations of principal targets, which will likely include corporate puppets, nominee entities or other alter egos, will seek to develop and analyse the following information:

- real property ownership and property values;
- luxury assets;
- intangible assets;
- mortgage information;
- liens;
- judgements;
- bankruptcies;
- history of addresses and phone numbers;
- relatives;
- involvement in past or pending law suits;
- criminal records search;
- lifestyle;
- key business, advisory and social contacts;
- background history;
- modus operandi;
- general psychological profile and "litigation psyche";
- key strengths and weaknesses;
- decision cycle (i.e. how fast one will have to move in order to move faster than the primary obligor to ensure success);
- preferred laundering typologies;
- identities of money laundering advisors or model builders; and
- likely preferred courses of action.

The location of assets may be a determinative factor in case management. For example, if the cost of prosecuting proceedings in a particular jurisdiction is so

[6] Available at: *http://www.bloomberg.com/news/features/2016-03-20/the-behind-the-scenes-fight-between-apple-and-the-fbi* [Accessed 28 October 2016].

prohibitive that even a successful recovery would yield little net benefit, a victim bank may elect to cut its losses, especially where the risks of an adverse costs award exist.

Regardless of where assets are located, it is nearly always advisable to liaise with local law enforcement. Useful intelligence may be available that could minimise or obviate the necessity for expenditure on investigations. In some cases, it may be possible to co-operate with local law enforcement and government agencies to secure a recovery without even the need to initiate proceedings.

Other evidence gathering methods include interviewing individuals, innocent or otherwise, connected to or potentially possessing useful information regarding the crime. Such interviews must be undertaken with great caution, especially of parties who are known or suspected to be accomplices. The potential value of probing for evidence must be weighed against blowing cover or prematurely undermining the strategic advantage of investigative secrecy. There are manifold ways in which to conduct evidence-gathering interviews. Typical best practices include avoiding "formal" interrogations; often, a cloaked "fishing exercise"—conducted in the right situation and in the right manner, understanding what questions to ask and how to ask them without arousing suspicion—will yield vital clues about a suspect without their even being aware. Likewise, accomplices can unwittingly volunteer useful information when they are presented with no consequences to fear. Such covert intelligence and evidence gathering frequently yield more valuable material than official interviews or discovery. Generally speaking, people like to talk and many like to brag, becoming acquainted with the perpetrator's hunting grounds and establishing contacts in his relevant spheres of influence can also provide opportunities for harvesting important information. Fraud cases are notoriously complicated and puzzle-like. Even seemingly innocuous fragments of intelligence or information could have significance once a more complete picture comes into focus.

Conducting certain types of information gathering under cover of secrecy is vital in circumstances where court or other official intervention or assistance is required. Where it is necessary to seek the assistance of a court in gaining access to information, it is critical to ascertain whether the jurisdiction of that court encompasses ex-parte procedure designed to uncover information under seal. Not all jurisdictions are amenable to granting this type of relief. Certain civil law jurisdictions (which include the designated secrecy locales of Belgium and Luxembourg), for instance, do not recognise such procedures. If a particular jurisdiction's legislation does not specifically provide for the use of ex-parte procedure, recourse may be found under the rules of civil procedure. Most common law-based courts have jurisdiction to hear a variety of applications without notice and appeal can be made to the "inherent" jurisdiction of a court to do as it sees fit to ensure that the ends of justice are met. In general, the common law jurisdictions, including the US, the UK and Australia, provide for broad reliefs in such contexts.[7]

Where the target of an information gathering exercise is a bank court or official, information gathering channels will invariably be involved. Banks process millions of transactions every day. Many involve third-party funds or assets, such as, for example, accepting deposits, receiving loan repayments and accepting loan collateral. The vast majority of bank transactions are ordinary and legitimate. Accessing the right information can be like searching for the proverbial needle in the haystack. How do we parse the good from the bad? Hundreds of millions of dollars of illegal transactions run through the banking system every day. These can range from a simple forged check to entire systems of money laundering and financial fraud committed through multiple wire transfers. Many of these transactions bear no distinguishing feature, and certainly none will be explicitly stamped "illegal!" but others may raise red flags. Considerable expertise and experience are required to cull wheat from chaff.

Accessing this information can be costly and time consuming. So how does one gather the necessary evidence? If the name of an account holder is known there are many ways in which pertinent account information can be accessed. The manner in which information is accessed will depend on: (a) whether the requesting party is a private individual or an arm of the State; and (b) the location of the bank. As a general rule, there are many more facilities afforded to an arm of the State than to a private individual when seeking to gather bank records. For example, if a criminal investigation is underway in which *significant* money laundering activities are suspected, a foreign jurisdiction may seek information from the US Financial Intelligence Unit (FIU) —the Financial Crimes Enforcement Network (FinCEN) —through a procedure referred to as a 314(a) Request (or a FINCEN "blast") in order to determine whether an individual, entity or organisation maintains an account in a US financial institution. Upon receipt of a 314(a) Request, US financial institutions are required to search their records to determine whether they maintain any current account for each named suspect or any account maintained for a named suspect during the 12 months preceding the request. In addition, each receiving financial institution must also search its records for any transaction conducted by or on behalf of a named suspect and any transmittal of funds in which a named suspect was either the transmitter or the recipient within the six months preceding the request. If the prerequisites are met, this is a powerful information gathering tool. If not, there are other possibilities. US federal law empowers courts to permit any interested party to obtain discovery for use in

[7] For example, the US courts provide for broad ranging discovery powers, they also recognise an inherent power to seal a court's record, as the court in *Estate of Hearst* (1977) 67 Cal. App. 3d 777; 136 Cal.Rptr. 821 stated: "Clearly a court has inherent power to control its own records to protect rights of litigants before it, but 'where there is no contrary statute or countervailing public policy, the right to inspect public records must be freely allowed'. [Citation.] … [Countervailing] public policy might come into play as a result of events that tend to undermine individual security, personal liberty, or private property, or that injure the public or the public good."

foreign proceedings from a person located in the district, even if this evidence could not be accessed under the rules of the foreign proceeding.[8] 28 U.S.C s.1782(a) does not impose a foreign discoverability requirement nor must the foreign proceeding actually be pending. Section 1782 requires only that the discovery be useful.

While the process of obtaining evidence from banks not situated in the US is, generally speaking, not as straightforward, if a foreign bank has a branch in the US the 314(a) Request (31 CFR Pt 103.100) can also be used against that agency or branch, as the s.314(a) regulations apply to all "financial institutions" as defined by the Bank Secrecy Act.[9] In the civil context, the US District Court for the Southern District of New York has heard many applications for discovery of bank records of foreign banks with a branch in New York.

Information gathering should take place simultaneoulsy with real time analysis. Dedicated information analysts can play an important role in both crafting and guiding the information gathering process. Likewise, information gatherers can often offer tales from the field that put a different gloss on a particular fragment of information which will assist analysts in developing a clearer or more in-depth understanding. The dual and concurrent processes of gathering and analysis must be harmonised and synthesised. Where information has been obtained under court mandated seal, analysts must work with precision and speed to ensure that a comprehensive picture has been formed by the time the permitted seal lapses to enable appropriate relief to be sought, such as, for example, to secure assets.

Preserve evidence

Evidence preservation is important enough to warrant further elaboration beyond the brief comments offered above. Digital evidence preservation is primarily concerned with maintaining integrity and, thereby, its value for use in court proceedings. Contaminated evidence is for all intents and purposes valueless. Explanations offered to a court as to how contamination took place and how it may or may not affect the quality of the evidence will usually fall on deaf ears. The importance of preservation cannot be overemphasised. Even a whiff of doubt regarding the integrity of an item of evidence can jeopardise the success of an entire investigation.

Evidence preservation can also refer to the maintenance of secrecy during the course of an investigation as a means of preserving the value of evidence already obtained but which would (or could) be compromised by disclosure. In this regard, operational and budgetary risk management are important aspects of preparing an investigation and recovery plan. Steps must be taken to preserve the operational security (OpSec) of work proposed or in-motion. Such steps might include source protection and communication security as part of case management and reporting. Other measures that can be employed in conjunction with disclosure orders include sealing and anti-tip off (also known as gagging) injunctions. Gagging injunctions will direct the court's registrar (or clerk) to seal the court's record of the application and prohibit the targets of discovery, the banks, from disclosing: (1) the fact of the disclosure order; (2) its contents; or (3) the fact of compliance with the order, to any person save for counsel. Counsel is similarly restrained. This form of relief will have a major positive impact on the tracing process and preserves the status quo until such time as sufficient evidence has been gathered to enable a freezing order or similar relief to be applied for and obtained. The process of denying information to adversaries involves identifying, controlling and protecting the outward signs or indicators associated with the process of investigation.

Preserving electronic evidence involves a special set of considerations. Computer operating systems and software programs frequently add, delete or alter the contents of electronic storage devices. This can occur automatically without user command or awareness. Where digital evidence is to be produced in court, just as with documentary evidence, the onus is on the party offering that evidence to show that it is exactly the same as that taken into possession by the evidence gatherer. It is therefore critical to establish a comprehensive, unimpeachable preservation protocol so as to be able to attest to an inviolate chain of custody. Objectivity, continuity and integrity of evidence must be demonstrable. It is also crucial to be able to demonstrate how evidence has been recovered, showing each step or stage of process by which the evidence was obtained. The process of preservation and results presented to the court must be precisely duplicatable by a third party.

A plan of evidence preservation is an integral part of any successful asset recovery strategy. Each case will have unique features and considerations that will stimulate particular preservation concerns and thus require dedicated measures to ensure that provenance is clearly demonstrable and integrity guaranteed. As the success of an asset recovery strategy can stand or fall on the quality of evidence, a purely reactive approach is untenable. It

[8] 28 U.S.C. s.1782 (U.S. Code Title 28 Pt V Ch.117 s.1782—Assistance to foreign and international tribunals and to litigants before such tribunals).

[9] Bank Secrecy Act 18 U.S.C. s.5312(a)(2). "Financial Institutions" in that section include: (a) an insured bank (as defined in s.3(h) of the Federal Deposit Insurance Act (12 U.S.C. s.1813(h)); (b) a commercial bank or trust company; (c) a private banker; (d) an agency or branch of a foreign bank in the US; (e) any credit union; (f) a thrift institution; (g) a broker or dealer registered with the SEC under the Securities Exchange Act of 1934 (15 U.S.C. ss.78(a) onwards); (h) a broker or dealer in securities or commodities; (i) an investment banker or investment company; (j) a currency exchange; (k) an issuer, redeemer, or cashier of traveler's cheques, cheques, money orders, or similar instruments; (l) an operator of a credit card system; (m) an insurance company; (n) a dealer in precious metals, stones, or jewels; (o) a pawnbroker; (p) a loan or finance company; (q) a travel agency; (r) a money transmitter; (s) a telegraph company; (t) a business engaged in the sale of automobiles, airplanes and boats; (u) persons involved in real estate closings and settlements; (v) the US Postal Service; (w) an agency of the US Government or of a state or local government carrying out a power or duty of a business described in s.5312; (x) a casino, a gambling casino, or gaming establishment with an annual gaming revenue of more than $1 million annually; (y) any business engaging in an activity the Secretary determines by regulation to be similar to, related to, or a substitute for any business described in s.5312; and (z) any other business designated by the Secretary whose cash transactions have a high degree of usefulness in criminal, tax or regulatory matters.

is vitally important that an evidence preservation protocol be developed and all eventualities thoroughly considered at the outset.

Develop and implement strategy

Just as an ounce of prevention is worth a pound of cure, an ounce of strategy is worth a pound of remediation. In asset recovery, strategy is paramount. Strategic planning, simply put, is a systematic process of envisioning an end result, translating that vision into broadly defined goals or objectives, and plotting a sequence of steps to achieve them. Conducting a far-reaching asset location and recovery exercise requires the preparation of a comprehensive map of objectives and a plan of action. Upon discovery of fraud, the first task is to define the overarching objective of any proposed asset recovery attempt and then break that down into subsets linked to various probable scenarios and intermittent outcomes. This process will necessarily involve an analysis of the means available to achieving various ends, routes to be taken and potential for compromises in a variety of likely situations. The overall objective cannot be viewed in isolation from the route towards that goal or as divorced from the potential obstacles along the way. The importance of early focus and analysis on key issues cannot be overstated, it will reduce needless or futile expenditure of human and financial capital and will sharpen focus on defining staged intermediate objectives.

A well thought out and developed strategy is a blueprint for success in most endeavours. This is particularly important in asset recovery operations, given the ingenuity and adaptability of many white-collar criminals and the many variables in fraud matters. Development and implementation of strategy involves more than just a commitment to planning, however. Effective strategy requires an overarching comprehension of how to practically execute those plans.

Strategies which aim for the unachievable are valueless. Tactical plans must be realistic and attainable. To succeed, the process must function optimally, and investigation and recovery professionals should have clear success markers to guide forward trajectory, bolster confidence and encourage perseverence. While each fraud case presents unique circumstances and rules of engagement, nearly every matter will reference or draw from a playbook of established strategic precepts. These include a clear, shared vision, an understandable concept and a well-defined route to an agreed end result. Radiating from that core, good strategy also involves separate tactical strands engaged as appropriate depending on which professional discipline is called for in any given moment or situation.

Development and implementation of effective strategy requires collaborative team work under strong leadership. One manager should have oversight and responsibility for the cross-pollination and assimilation of ideas and then guide translation into a format easily understandable for all tasked with execution. Responsibility for implementation is best delegated according to expertise and experience. For example, the investigative plan requires focused tactical decision making grounded in field experience; the litigation plan involves similar skills but honed in different circumstances and, accordingly, deployed to achieve distinct case-specific aims.

Each asset recovery matter requires its own case-specific strategy. Strategic planning serves as a framework for management decisions and a guide to the realisation of the overarching objective, as well as a basis for benchmarking and performance monitoring. Strategy development should not be a rigid, box-checking exercise, however, it is a process. It requires core team agreement on essential decisions and the criteria for making them. Even a well thought out and seemingly comprehensive strategy will be all but hobbled if those tasked with implementation do not fully understand it or are unprepared to execute it.

Management theorist Henri Fayol identifed planning as one of the prime responsibilities of management. He defines planning as "examining the future, deciding what needs to be done and developing a plan of action".[10]

Strategic planning begins with an objective and works backwards. At every stage of a strategic plan, the means to achieve the next objective or step along the path must be identified. Situation analysis and goal identification represent the opposite ends of the strategy continuum; all stages in between are fluid. Accordingly, adaptability is equally important. Force-field analysis is a management technique developed by Kurt Lewin, a social science pioneer, for diagnosing situations. It is useful when looking at the variables involved in planning and implementing a change programme and can be beneficially applied to the variables involved in an asset recovery operation. Pre-identification of potential force-fields allows for developing contingency plans that can be integrated into the overall strategy if and when a situation calls for it. In this way, what might have been a rock in the river bed becomes a pebble, significantly diminishing the possibility that an entire plan might founder due to any single miscalculation.

Fluidity is critical throughout the process of development and implementation. At each sub-stage, it will be necessary to monitor and evaluate progress and review or adapt the overall strategy. Monitoring and evaluation links strategy to implementation but can only be successful if considered at the outset, such that baseline data for each indicator has been collected and success can be monitored against this data.

The formulation of any strategy requires, at first instance, an answer to the question "what is the objective?" and, secondly, a consideration of how to reach the end result. This necessarily requires an ongoing evaluation of all considerations at play, including the personality types involved, how they interact between

[10] B. Burnes, *Managing Change: A Strategic Approach to Organisational Dynamics*, 5th edn (Harlow: Prentice Hall, FT, 2009), p.40.

and among each other and within their environs, and how they respond to different stressors or incentives. This is as applicable to the asset recovery team as it is to the adversary. True team strength and unity derives from cohesion around a common mission, set of guiding principles, central focus and agreement about team culture to be practiced and accepted by everyone. To that end, the asset recovery team's strategy must take account of external factors as well as be custom-tailored to the abilities and qualities of all team members. Finally, effective communication—regarding strategic vision, expectations and actionable milestones—is essential to successfully moving the matter forward.

Reputational fall-out

Earlier, we touched on the topic of reputational "fall-out" following a company discovering it has become a victim of fraud. While gathering and preserving evidence is a vital first step following discovery, the rush to protect reputation and manage bad publicity has taken on a new dimension, particularly in the years following the economic crash of 2007–08. Many banks took severe reputational blows as a result of negative publicity and loss of confidence in the banking system as a whole. This only amplified many bank leaders' first instinct following the discovery of fraud: "self preservation" (or reputational salvage) over devising sensible, temperate solutions to address the acute larger problem. This form of response is more often than not detrimental both to the institution itself as well as to a wider class of affected parties.

Consider the case of Deutsche Bank (DB). DB failed to recognise up to US $12 billion of paper losses during the financial crisis. What could the motivation for such an action have been? Three former bank employees alleged that if the Bank had properly accounted for its positions—estimated at US $130 billion on a notional level—its capital would have fallen to dangerously low levels during the financial crisis and it might have required a government bail-out to survive. During the financial crisis, many financial institutions faced existential threats to their very existence. According to the complaints made to the SEC by former employees, DB, motivated by self preservation, substantially inflated the value of its credit derivatives portfolio; it was not alone in making that nature of maneuver. Self preservation will continue to drive financial institutions to do irresponsible things rather than face the music and take the blame. So long as bank leaders are immune from personal repercussions, there appears to be little impetus for them to place broader social and economic interests before those of the institution whose reputation they are driven to preserve.

To be clear, we make no suggestion that bank leaders ought to minimise or ignore reputational fall-out. The issues are of balancing priorities and upholding corporate social responsibility as a genuine code of institutional behaviour, not merely PR window-dressing. Misconduct at banks imposes costs on society over and above the hard costs to those directly affected. A loss in confidence in the financial system affects not just that system but all other related systems and, ultimately, the economy as a whole. When a bank has been visited by fraud or other scandal it is vital that management set in train not just a program of recovery but also a program of reputational damage mitigation. Share values can plummet upon wind of wrongdoing or other irregularities; hence, the importance of establishing an information management crisis protocol alongside the recovery programme. Crisis communications experts, working in concert with in-house legal counsel and senior management, should be authorised to interact with media outlets and various interested stakeholder agencies to properly respond to enquiries and carefully moderate institutional responses, social media and other information outflow. Stemming potentially damaging information flows is important both for stabilising the institutional crisis but also toward assuaging broader concerns or anxieties which could potentially trigger a downward spiral among other stakeholders and sectors.

The preponderance of commentary on banking misconduct and regulatory bodies has focused on the consequent costs borne by the banks, rather than those foisted onto society. The costs to financial institutions are readily identifiable in the form of fines and provisions. The costs to society are immense but far less easy to quantify. One credible attempt is a report issued by the European Systemic Risk Board on misconduct risks in the banking sector.[11] Two dimensions of the potential systemic impact of misconduct by EU banks, analysed from a macroprudential perspective, are identified. The report categorically notes that misconduct at banks imposes costs on society. In particular, it damages confidence in the financial system, which is a vital element for the proper functioning of the economic system as a whole. Secondly, the report suggests that while financial and other penalties applied in misconduct cases can serve as a correcting mechanism, these penalties may, in certain cases, also entail independent systemic risks that could impose costs on financial system users. Misconduct and related penalties are typically tail events which can create uncertainty about banks' business models, solvency and profitability.

There seems to be little question that society's perceptions of the banking sector has been badly degraded as a result of the economic crisis, but the acts of bank leaders when faced with fraud at an institution can lead to a further loss of confidence if not managed properly. An unprincipled race to preserve face can do far more harm than good in the long term. Crisis mitigation and response protocols must entail management of public relations but also immediate loss assessments and

[11] European Systemic Risk Board, *Report on misconduct risk in the banking sector* (2015) available at: *https://www.esrb.europa.eu/pub/pdf/other/150625_report_misconduct_risk.en.pdf* [Accessed 28 October 2016].

recovery strategies coupled with a willingness to bear responsibility for faulty decision making and a pledge to learn from mistakes made.

Conclusion—profitability and the greater good

The pressure for profitability in international banks continues to drive many management decisions. Now that the worst effects of the financial crisis appear to have subsided, pressure is increasing in international banking to:

- post better financial results on a quarterly basis (or monthly basis among some banks which are under above-normal scrutiny by government agencies);
- compete more successfully;
- move into new offshore markets; and
- complete offensive or defensive mergers and acquisitions driven by quasi-monopolistic or cost-cutting objectives.

Senior officers and directors have little choice but to deliver on these expectations. One recent trend is to expand the area of influence of chief financial officers (CFOs) to be more than the traditional "Mr or Ms No" regarding spending on new initiatives. A positive perspective on that is that CFOs are increasingly included as part of the strategic team at banks; a more pessimistic slant is that those CFOs are now also under pressure to "build value" for investors.

We referred above to the example of Royal Bank of Canada, noting how its aggressive drive to attract high net worth customers in Latin America led to poor risk-management decisions. A worse and still unfolding, example of what can happen when banks try to build their "books of business" at all costs is the notorious bribery scandal at Petrobras, the Brazilian national oil and gas company. Approximately 30 Swiss banks, holding some 300 distinct accounts, are being investigated in connection to banking transactions with parties connected to Petrobras.

In Pt I of this article, we also discussed the importance of rebuilding trust in the banking sector. Trust cannot be regained by pushing for profits at all costs. If the global economic downturn has taught nothing else, it is that that model has no future. While the ongoing necessity of continual innovation often manifests itself in efficiencies that increase value and profit, bank leaders must grapple with the new reality: fairness and equity over the long term for all stakeholders.

Writing about global corporations in a Harvard Business Review article, Harvard Business School Professor Michael Porter proposed that

> "businesses must reconnect company success with social progress … Shared value is not social responsibility, philanthropy, or even sustainability, but a new way to achieve economic success. It is not on the margin of what companies do but at the center".[12]

Corporate social responsibility has become a buzz word in the community of global enterprise. Over the years, it has evolved from corporate philanthropic giving and charitability programs to a complex set of principles governing almost every interaction a company has with society. According to a statement from the Corporate Social Responsibility Initiative (CSRI) at Harvard's Kennedy School of Government, "corporate social responsibility encompasses not only what companies do with their profits, but also how they make them".[13] Continuing, the CSRI suggests that

> "it goes beyond philanthropy and compliance and addresses how companies manage their economic, social and environmental impacts, as well as their relationships in all key spheres of influence: the workplace, the marketplace, the supply chain, the community and the public policy realm".

For leaders and directors solely focused on driving profit at any cost, the idea of "the greater good" is a proverbial thorn in the side. They would argue that profits are not furthered by policies or business models which place a premium on corporate social responsibility nor will they accept that in many cases, in fact, profits suffer. However, researchers from Harvard Business School, University of California and the University of Michigan conducted a joint review of 167 scholarly studies on the topic of corporate charitable contributions, their conclusions, as quoted in a paper entitled *Measuring the Value of Corporate Philanthropy: Social Impact, Business Benefits and Investor Returns*, were that

> "after thirty-five years of research, the preponderance of scholarly evidence suggests a mildly positive relationship between corporate social performance and corporate financial performance and finds no indication that corporate social investments systematically decrease shareholder value".[14]

Taking this to be the case, there should be no real impediment to the finance industry working to combine maximisation of shareholder wealth with societal development. In ways meaningfully different from other types of global corporations, banks bear a great responsibility to society. This appears to have been all but forgotten in the dogged pursuit of profit. While the profitability of corporate social responsibility generates

[12] M. Porter and M. Kramer, "Creating Shared Value" (2011) 89 *Harvard Business Review* 62–67.
[13] CSRI, *Corporate Social Responsibility as Risk Management: A Model for Multinationals*, Working Paper No.10 (2004), p.9 available at: *https://www.hks.harvard.edu/m-rcbg/CSRI/publications/workingpaper_10_kytle_ruggie.pdf* [Accessed 28 October 2016].
[14] Terence Lim, *Measuring the Value of Corporate Philanthropy: Social Impact, Business Benefits and Investor Returns* (New York: CECP, 2010) available at: *https://philanthropynw.org/sites/default/files/resources/MeasureValueCorpPhilanthropy-2010CECP.pdf* [Accessed 28 October 2016].

considerable disagreement in certain quarters, most business leaders appear in accord that corporate citizenship is no longer a choice but a requirement.

In a report authored by Ernst & Young, a global consultancy and accountancy firm, entitled *Global Banking Outlook 2015: Transforming Banking for Next Generation*,[15] the authors argue that banks will need to reinvent themselves in the next decade—not just to respond to the pressures of today, but to be flexible enough to adapt to the world of tomorrow. The Report concludes by predicting that ten years from now, the leading banks will not necessarily be defined by their products and services or even by the most efficient operations. While they will be assessed by those deliverables, they will be defined by their ability to manage the risks of change programs and to make the right investments in products and services. They will be defined by their ability to create an internal culture that weds dynamism to best practice. They will be defined by their ability to deliver new fit-for-purpose business models. Speaking about the initiative that puts social values before profit, Marcos Eguiguren, Executive Director of the Global Alliance for Banking on Values, declared that "there is a huge difference between having profitability as one of our goals and having it as a consequence of doing things properly".[16]

The time is ripe for a culture change in banking—not only with respect to managing risk but also from the perspective of creating profit. Banks that fail to manage this cultural transformation will suffer in the long term. The only sustainable business model is one that will still generate profits but which also encourages employees to do the right thing.

[15] Available at: *http://www.ey.com/Publication/vwLUAssets/ey-global-banking-outlook-2015-transforming-banking/$FILE/EY-global-banking-outlook-2015-transforming-banking.pdf* [Accessed 28 October 2016].
[16] Jennifer Jacobs, "Banking on the Right Values", *Personal Wealth: The Edge Malaysia*, 25 February 2016.