

Trust and occupational fraud

How to trust is just as important as who to trust.

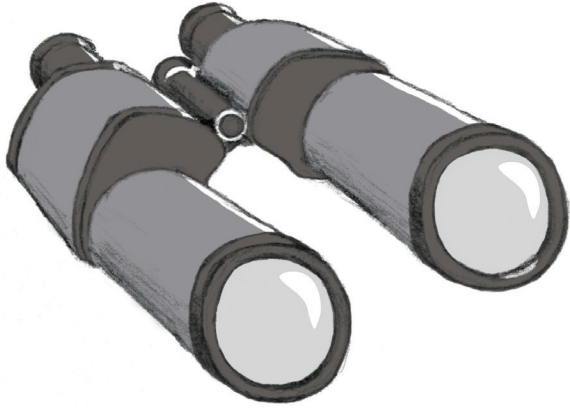
A Grant Thornton white paper

Trust is one of the most important and complex issues facing Canadian companies today.

While trust within an organization is clearly necessary for employee satisfaction, efficient business operations and the resulting competitive advantages these provide, it can also create the potential for fraud, which in extreme cases can result in bankruptcy.

Understanding how trust relates to or leads to fraud is actually quite complicated. How do businesses determine when and where too much trust has been bestowed, and how can they determine when and how trust has been breached? Trust-related fraud by its nature involves subjective, often imperceptible, human processes, which makes it difficult to deter, detect and deal with. In fact, the *Report to the Nations on Occupational Fraud & Abuse—2010 Global Fraud Study* notes that “the inherently clandestine nature of fraud means that many cases





will never be revealed, and, of those that are, the full amount of losses might not be uncovered, quantified or reported.”¹ It’s a particularly challenging issue for privately held businesses that may not have the same levels of fraud prevention and detection controls as larger, public companies, or who may not fully appreciate the impact trust-related fraud can have on businesses of all sizes.

The fact is, fraud is very often a function of trust, or more specifically, of the levels of trust and corresponding controls that are assigned to an organization’s various roles—CFO, accountant, manager, clerk, etc. Understanding who to trust (people) and how to trust (controls) are therefore critical steps in the development of any fraud prevention initiative.

The background picture—where to focus

There are differing theories about how organizations should handle trust. Recent approaches suggest that organizations aren’t placing enough trust in their employees and that the feeling of being more trusted makes employees more productive. There may be considerable truth to this, but the flip side that organizations should consider is that employees who have been allocated high levels of trust are still quite capable of committing fraud, are actually very well positioned to do it, and often do become perpetrators.

- The majority of occupational frauds are committed by employees and managers [with fraud by managers resulting in greater financial loss to the company].²
- More than half of all cases were committed by individuals between the ages of 31 and 45. Generally speaking, median losses tended to rise with the age of the perpetrator [peaking with the 56-60 age group].³

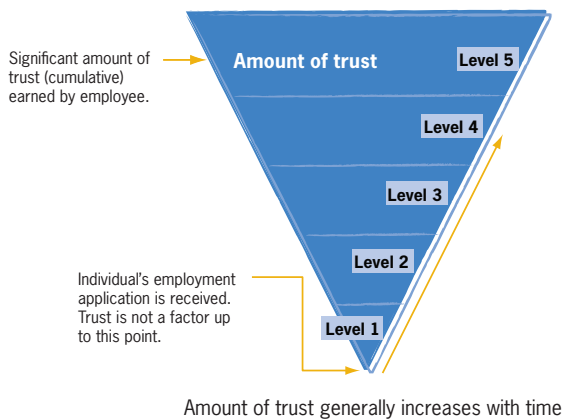
¹ The Association of Certified Fraud Examiners, *Report to the Nations on Occupational Fraud & Abuse—2010 Global Fraud Study* (Austin, TX: The Association of Certified Fraud Examiners, Inc., 2010), 8.

² ACFE, *Report to the Nations—2010*, 48.

³ ACFE, *Report to the Nations—2010*, 56.

As these statistics suggest, seniority and experience—both of which, more often than not, indicate higher trust levels in the individual—actually result in an increased incidence of fraud. If employees who have achieved higher levels of trust actually commit fraud more often, it follows that the notion of extending greater trust to employees in general must be tempered and qualified.

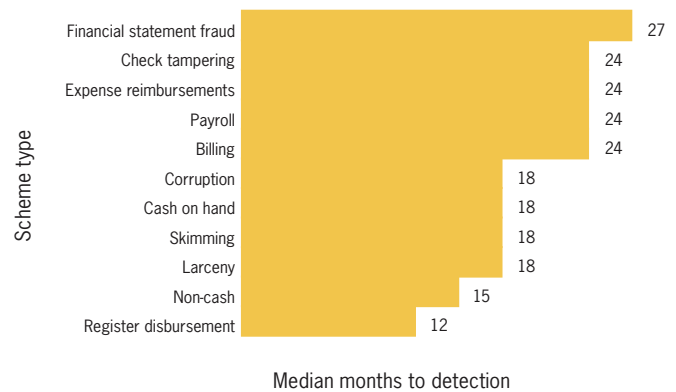
Inverted triangle of trust



Consider the case of an office manager who defrauded her company of a considerable sum. An investigation determined that virtually no controls were placed on her or her activities within the company due to her long-standing employment with the company and the complete trust placed in her by the owner as a result of their personal relationship. This fraud, which occurred over an extended period of time and amounted to approximately \$600,000, might have been detected or deterred by the implementation of simple verification controls.

Fraud schemes succeed by leveraging trust over many months or even years, allowing financial loss to mount undetected:

Median duration of fraud based on scheme type⁴



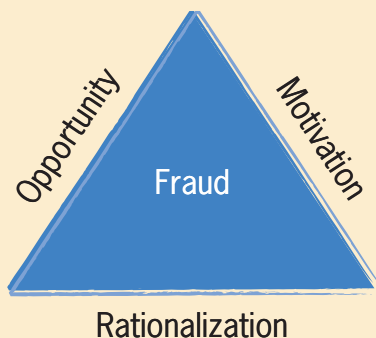
Organizational trust requires a balance between subjective relationships and objective controls, and there can be repercussions to placing too much trust on either side. With this premise in mind, we will examine these two essential components of trust—people and controls—and consider how trust is assigned to each.

⁴ ACFE, *Report to the Nations—2010*, 14.



People—the most unpredictable investment

Is there any way to account for the seemingly contradictory nature of trust in organizational structures, where long-standing employees get trusted more, despite committing a large percentage of frauds as well as the most costly? One approach is to consider how trust can be reflected in the elements of the Fraud Triangle, a diagram traditionally used to depict the combination of factors that are needed for an individual to commit fraud:



It's easy to see how each factor can arise from a trust issue:

- Opportunity—There are no controls in place; the organization relies on trust.
- Motivation—An individual feels the need to hide something in order to retain a position of trust.
- Rationalization—"I need to look after myself because I can't trust them to be fair."

Forensic accountants often cite a rule of thumb which holds that 80% of people are at least capable of an unethical or illegal act,⁵ so when these types of circumstances are aligned, most individuals do, in fact, have the capacity to commit fraud. Detecting potential perpetrators within an organization, however, is difficult because most of the factors that lead to such acts are psychological and may only be evident in their personal lives, if at all. They're often the people considered least likely, which makes detection particularly difficult for smaller businesses who consistently have "fewer controls in place than larger organizations," despite the "disproportionate impact of fraud on these companies."⁶

As anyone can attest who has gone into business with a trusted partner, only to be subsequently defrauded or financially manipulated, people can end up being the riskiest part of an investment. The pressures and influences on any individual are substantial, varied and hard to quantify: personal circumstance, the economy, individual morality, even human nature. When any combination of these is at work, the boundaries of trust are inevitably pushed or broken, and the capacity of individuals to commit fraud is transformed.

Not only do external factors change—and they always change—but people change as a result. Consider this scenario: An individual with a gambling habit, not extensive but occasionally resulting in unforeseen debt, has their work hours cut in half when their employer scales back due to a difficult economy. Debt is high, income is reduced, guilt rises, desperation sets in—potentially, a basically good individual can be led toward committing a fraudulent act, and the level of trust they enjoy in their job may well determine the extent to which that fraud can be perpetrated.

⁵ Jeff Buckstein, "Speaking up can carry a high price," *The Bottom Line*, <http://www.thebottomlinenews.ca/index.php?section=article&articleid=364> (accessed May 31, 2010).

⁶ ACFE, *Report to the Nations—2010*, 39.

This is why the prevailing trend to just trust more—and to view owners or managers who insist on extensive controls as somehow “distrustful” of their people or their organization—is not only risky, but a questionable interpretation of what organizational trust really means. Management should not be taken to task for recognizing that unregulated trust is an unreliable business practice or for acting to mitigate risk through appropriate trust controls. In fact, taking these steps can be particularly hard and often unpleasant for owners of smaller businesses, given the inherent intimacy of owner-employee relationships in such organizations. But trust cannot function as its own control; you can’t be sure that things are being done properly just because employee A is in charge, and employee A is “completely trustworthy.”

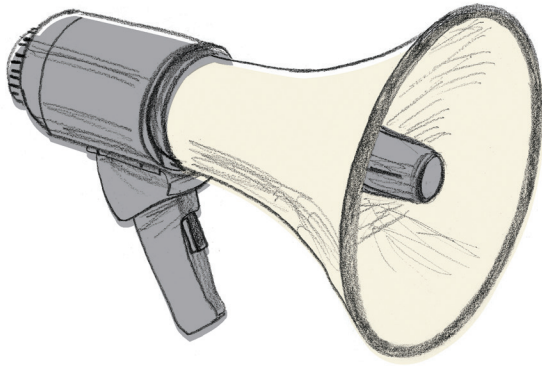
The granting of trust is clearly necessary for the efficient and harmonious operation of a business, but it also seems likely—if seniority and experience can be trust liabilities—that trust should actually be measured more closely, validated more often, earned more demonstrably and withheld more frequently. It shouldn’t be bestowed out of friendship, loyalty, tenure, experience, or simple lack of organizational rigour. Trust can’t be implemented simply because a prevailing theory says more is better, and it can’t be upheld just because an owner or manager doesn’t want to appear distrustful or is uncomfortable withdrawing trust from a colleague. It can be granted to new hires provisionally, as justified by adequate background and reference checks, but—since the ACFE reports that of all the perpetrators studied, “eighty-six percent had never been charged with or convicted of a prior offense”⁷—those trust allocations must also be regularly managed and re-evaluated by the rigorous application of controls. The idea is not just to trust more, but to build a culture of trust that permeates the organization, where trust is carefully allocated as part of an

inclusive risk management strategy and is therefore more meaningful when earned and more potent as an influence on behaviour.

You can take a basic systematic approach to help ensure that employee trust levels are justified and subsequently validated:

- Measure levels of trust bestowed.
- Determine how much risk derives from reliance on trust.
- Modify current levels of trust based on risk tolerance.
- Increase trust going forward based on a “trust earned/demonstrated” model.
- Add periodic trust validation steps.
- Adjust as necessary.

⁷ ACFE, *Report to the Nations—2010*, 69 .



Controls—the best way to steer trust

Some business owners may rely on internal accounting procedures to discover fraud, but those procedures are also often the source of it. External accounting procedures such as audits or fraud probes are more likely to uncover fraud, but this is often after the fact and after a lot of damage may have been done. So while there's no accounting procedure to completely prevent fraud or absolutely validate allocated trust, you can implement trust controls throughout all organizational procedures and systems, especially in danger spots such as accounting and IT.

Begin by determining where you're placing excess trust. Watch for red flags indicating individuals whose trust levels are too high or who should have increased controls applied to their areas of responsibility. Be aware of employees who, for example,

- are living beyond their means,
- are experiencing financial difficulties,
- display a wheeler/dealer attitude,
- have control issues, and/or
- have unusually close associations with vendors.

Once these red flags have been analyzed, you can apply controls to revise trust levels throughout the organization as well as for specific individuals. Controls include

- hotlines,
- surprise audits,
- fraud training for employees,
- employee support programs,
- job rotation/mandatory vacations,
- segregation of duties to reduce the extent of fraud committable by one person,
- redundant transaction authorization,

- limited access to sensitive areas,
- client or vendor visits to verify authenticity of transactions, and
- documentation reviews.

- **Tips are the number one means by which fraud is detected. However, less than half of the victim organizations in our study had a hotline in place at the time the fraud occurred.⁸**
- **Hotlines were the control with the greatest associated reduction in median loss.⁹**

There are also numerous trust controls that apply specifically to IT systems and issues, including controls to manage system integrity and data security, as well as controls embedded within specific business process applications. Organizations would be well-served to invest in IT fraud prevention and detection services, since the monitoring and verification of these controls is so crucial, as is the implementation of trust-related controls for the individuals who wield the specialized, selectively understood knowledge that constitutes an organization's IT network.

It's imperative, however, that organizations not be lulled by a false sense of security because they believe controls alone provide independent certainty. It's not that controls themselves are unreliable, but that an overreliance on them leaves you

⁸ ACFE, *Report to the Nations—2010*, 38.

⁹ ACFE, *Report to the Nations—2010*, 42.

vulnerable on those occasions when they're ignored, not applied, applied incorrectly, circumvented, breached or are simply not working as designed. It's also important to remember that **trust itself is not a control; trust must be controlled and verified**. In organizations where upper managers have achieved a level of high—if not complete—trust, fraud is a real danger, either from that manager committing the fraud or because they are not properly carrying out the duties that they have been so absolutely trusted with—trusted to the point that their work is not being further verified by any controls whatsoever.

Other “controls” that can lead to an unjustified sense of security are current perception and past history: the fact that you don't see anything wrong now and don't have evidence of anything having gone wrong in the past is not in any way a control for future risk. Things change; more importantly, people change as their work and personal environments evolve due to new motivators/pressures, rationalizations or opportunities (both real and perceived).

The balancing act—Would you trust this man? Or this measure?

The best way to achieve a true culture of trust is to implement comprehensive controls designed to limit

- **undue trust**, where too much trust is placed in one person or one process/control;
- **misplaced trust**, where the wrong person is trusted; and
- **abuse of trust**, where trust is initially legitimately bestowed, but then breached by an individual whose relationship with the company has surreptitiously changed or been corrupted.

Undue trust shouldn't be an issue if duties and responsibilities are appropriately limited and segregated and if controls are comprehensive, effectively distributed across the organization and actually operating effectively. Misplaced trust can be

tempered by proper background and reference checks, but even when someone is trusted who never should have been, controls that limit responsibility and verify completed work can cut this trust issue short before much damage is done (though the initial risk can never be completely eliminated). Abuse of trust is the most challenging issue to address, as it often involves someone who was, in fact, initially perceived to be trustworthy—perhaps relied on heavily by the owner—but who underwent a change over time due to any number of unpredictable factors. The rigorous and comprehensive application of internal controls is the most effective way to circumvent and hopefully limit this sort of problem.

Of course, human nature cannot be controlled, and no controls can ensure that fraud will not be committed. Organizations must engage in something of a trust balancing act between people and controls, where excessive trust is not placed on either side. With individuals this is wise because of the impossibility of accurately predicting behaviour under ever-changing personal pressures and circumstances; when controls are not being applied or are not functioning properly, the solution can often be further controls, but regardless of the level of redundancy, the effectiveness of controls should always be periodically assessed and verified. In the end, the verification step itself is a crucial control.

Building a culture of trust

Despite substantial evidence that the mishandling of trust within an organization can lead to serious financial loss and even bankruptcy, senior managers and owners seem shockingly willing to take the risk, placing too much trust in their employees without verification and remaining generally uninterested in implementing fraud prevention and detection services and solutions. But everyone in the corporate picture pays when unregulated trust results in fraud. The potential for damage is large—morale, job loss, downsizing, stakeholder pressure—and usually leads to more organizational distrust than ever.



Perhaps a new way of looking at the problem is required, even an alternative terminology. Trust-related anti-fraud services would be more appealing to owners if they understood that “consistent verification” of roles rather than “complete trust” in individuals is the cornerstone of effective organizational trust. Owners implementing these services would be seen, not as distrusting their people, but as building a “culture of trust” and maximizing the value of trust across the company. Employees would not only accept trust-based anti-fraud strategies, but demand them, if it were clear that it was in their own best interests to do so.

There is a bigger picture behind the “trust more” veneer, one that includes owners, managers and employees as mutual custodians of a broader concept of corporate honesty.

Whether the issue is repositioned in this light or not, the fact is that all businesses—particularly privately held businesses that may not have comprehensive controls in place—are at risk for trust-related fraud. It’s a complex web of issues whose

solutions lie in a combination of measures: maximizing your understanding of trust, knowing the statistics (and that they apply to your business), initiating appropriate controls for your business, “controlling” your controls. You can’t trust to luck or fate. That could cost you and everyone around you.

Contributors

Daniel Lafleche

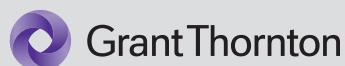
Forensic Accounting and Investigative Services
T (604) 443-2104
E dlafleche@GrantThornton.ca

David Elzinga

Forensic Accounting and Investigative Services
T (403) 508-1371
E delzinga@GrantThornton.ca

Raewyn Seeto

Assurance and Business Advisory Services
T (604) 443-2112
E rseeto@GrantThornton.ca



www.GrantThornton.ca

Audit • Tax • Advisory

Grant Thornton LLP. A Canadian Member of Grant Thornton International Ltd

About Grant Thornton in Canada

Grant Thornton LLP is a leading Canadian accounting and advisory firm providing audit, tax and advisory services to private and public organizations. Together with the Quebec firm Raymond Chabot Grant Thornton LLP, Grant Thornton in Canada has more than 3,100 people in offices across Canada. Grant Thornton LLP is a Canadian member of Grant Thornton International Ltd, whose member and correspondent firms operate in over 100 countries worldwide.

© 2010 Grant Thornton LLP. All rights reserved. We have made every effort to ensure information in this publication is accurate as of its issue date. Nevertheless, information or views expressed herein are neither official statements of position, nor should they be considered technical advice for you or your organization without consulting a professional business adviser. For more information about this topic, please contact your Grant Thornton adviser. If you do not have an adviser, please contact us. We are happy to help.