

Fraud busters

The hybrid work model, together with new financial pressures on businesses and individuals, have emboldened some employees to steal. Boards and regulators are responding with new standards and tighter controls, **Virginia Galt** writes

Le mode de travail hybride, tout comme les nouvelles pressions financières sur les entreprises et les personnes, en a poussé certains à voler. Conseils et autorités réglementaires répondent au défi avec de nouvelles normes et des contrôles plus serrés, écrit **Virginia Galt**



IN THE THREE YEARS since the global pandemic irrevocably changed the way work gets done, Canadian boards of directors – under pressure from external auditors – have been tightening their oversight of occupational fraud risks. The prolonged public health lockdown, which forced countries to switch to remote work, exposed weaknesses in organizations’ internal control systems. “The schemes got bolder and bolder,” says corporate director Alan Mak, national forensics practice leader at BDO Canada LLP and a member of the Chartered Professional Accountants of Canada board.

“It got kind of wild,” says Mak. The audacity was stunning. Some organizations fell victim to procurement fraud. “It was one thing [for procurement managers] to take kickbacks from suppliers, but we saw more than a handful of situations where procurement managers were ordering supplies that were never delivered and never existed.”

No sector is immune. The Government of Ontario, for instance, was scammed by an information technology director with access to the Education Ministry’s payment processing system. The employee recently pleaded guilty to embezzling \$11-million in pandemic aid funds intended to help parents with online schooling expenses. The funds had been diverted to bank accounts established under false identities.

Weak economy, strong incentive

While the nature of fraudulent activities may have shifted since then, the risk hasn’t abated, says Mak. Changing economic conditions – a strong recovery two years into the pandemic followed by high inflation and slower growth – have resulted in new pressures and temptations for employees to engage in theft, corruption and manipulation of financial results.

The widespread adoption of hybrid work arrangements, with employees alternating between on-site work and remote work, poses challenges for some organizations in terms of monitoring workforce activities. There is no evidence to suggest that the workforce is rife with thieves and fraud artists – a large majority of employees would never steal or abuse the trust of their employers, the Association of Certified Fraud Examiners says in its most recent international report on occupational fraud. But those who do commit fraud typically evade detection for 12 months before being caught, costing their organizations, on average, a 5-per-cent loss in revenue – and the losses can reach tens of millions of dollars depending on the magnitude of the scheme. The offences range from expense account padding – from the employee who bought cellphones for their entire family and charged it to the company, to the Ontario IT director who, in addition to pocketing pandemic aid funds, confessed that he had also taken \$36-million in kickbacks for computing services over the prior decade. He was sentenced to ten years.

Mak’s impression, from what he has observed in Canada, is that “fraud certainly seems to be on the rise, and attention or scrutiny by organizations on fraud risk is also on the rise.” In the past year, he said, there has been an uptick in the number of employees citing money pressures and the high cost of living as their reasons for crossing the line.

AU COURS DES TROIS ANNÉES écoulées depuis que la pandémie a changé nos modes de travail, les conseils d’administration canadiens – sous la pression d’auditeurs externes – ont resserré leur surveillance des risques de fraude en milieu de travail. Le confinement prolongé décrété par les organisations de santé publique, qui a forcé les pays à s’en remettre au travail à distance, a exposé les faiblesses des systèmes de contrôle interne des organisations. « Les complots de fraude sont de plus en plus audacieux, souligne l’administrateur Alan Mak, associé et chef national des services en juricomptabilité chez BDO Canada LLP et membre du conseil des Comptables professionnels agréés du Canada.

« Leur témérité était stupéfiante. Certaines organisations ont été victimes de fraude à l’approvisionnement. C’était une chose (pour les gestionnaires de l’approvisionnement) de toucher un bakchich des fournisseurs, mais on voyait aussi plus qu’une poignée de situations où les chefs de l’approvisionnement commandaient des fournitures qui n’étaient jamais livrées et n’avaient jamais existé. »

Aucun secteur n’est à l’abri. Le gouvernement de l’Ontario, par exemple, a été arnaqué par un directeur des technologies de l’information ayant accès au système de traitement de la paye du ministère de l’Éducation. L’employé a récemment plaidé coupable d’avoir détourné 11 millions de dollars d’un fonds de secours destiné à des parents faisant face à des dépenses scolaires en ligne.

Économie faible, puissante motivation

Même si la nature des activités frauduleuses s’est modifiée depuis, le risque n’en est pas moins toujours présent, explique M. Mak. Les conditions économiques changeantes – forte reprise deux ans après le début de la pandémie suivie d’une poussée inflationniste et d’une croissance faible – ont exercé de nouvelles pressions et tentations sur certains employés pour s’engager dans le vol, la corruption et la manipulation de résultats financiers.

L’adoption généralisée de modes de travail hybrides pose des défis à certaines organisations à l’égard de la surveillance des activités de la main-d’œuvre. Rien ne suggère que la force de travail soit truffée de voleur et de fraudeurs. Mais ceux et celles qui commettent ces méfaits échappent généralement à la détection pendant 12 mois avant d’être pris. Cela coûte à leurs organisations, en moyenne, une perte de cinq pour cent de revenus. Et ces pertes peuvent atteindre des dizaines de millions de dollars, selon l’ampleur de la combine. Les accusations vont du gonflement de notes de frais – de l’employé qui achète des téléphones intelligents à toute sa famille aux frais de la compagnie au directeur des technologies de l’information qui, en plus d’empocher des pots-de-vin pour des services informatiques, a aussi avoué avoir touché 36 millions de dollars de la même façon au cours de la décennie précédente. Il a été condamné à dix ans de prison.

De ce qu’il a observé au Canada, M. Mak retient que « la fraude semble certainement en hausse, alors que l’attention ou la surveillance par les organisations sont aussi en progression. » Au cours de la dernière année, dit-il, on a noté une hausse du nombre d’employés évoquant des pressions monétaires et le coût élevé de la vie pour expliquer pourquoi ils avaient franchi le pas.



Fraudsters typically evade detection for 12 months before getting caught, costing their organizations, on average, a 5-per-cent loss in revenue.

No sector is immune. The Government of Ontario, for instance, was scammed by an information technology director with access to the Education Ministry's payment processing system.
Aucun secteur n'est à l'abri. Le gouvernement de l'Ontario, par exemple, a été arnaqué par un directeur des technologies de l'information ayant accès au système de traitement de la paye du ministère de l'Éducation.

Tightening controls

New risks are always emerging, and “the bad guys are getting smarter and more sophisticated by the day,” says corporate director Benita Warmbold, an Institute of Corporate Directors Fellow and chair of the Canadian Public Accountability Board, the regulatory body that oversees the firms that audit publicly traded companies. CPAB is engaged with the International Auditing and Assurance Standards Board and Canada's Auditing and Assurance Standards Board on their current projects to revise fraud audit standards. At the same time, CPAB is holding Canadian audit firms under its regulatory watch to higher account in order to strengthen the quality of fraud audits and enhance the ability of auditors and, by extension, their clients to identify, assess and respond to fraud risks.

Fraud happens, but strong internal control frameworks can minimize the risks. Ideally, says Warmbold, “you want to catch it before it happens.” Failing that, the ability to move quickly to shut it down will reduce the damage.

In the corporate sector, external audit teams have incorporated fraud risk analysis into the annual inspections of their clients' financial statements. “Directors realize that fraud can have a serious impact on their finances and reputation and, ultimately, on capital markets in general,” says Warmbold, a chartered professional accountant who also serves on the boards of Bank of Nova Scotia, SNC-Lavalin and Methanex Corp.

The CPAB's fraud thematic review, published in May, 2022, provides an indication of the deeper scrutiny organizations can expect on compensation arrangements, the effectiveness of whistleblower programs, and whether they apply the fraud-risk lens as rigorously to managers as they do to employees. While organizations may be reluctant to question the integrity of managers, the CPAB notes that fraudulent financial reporting schemes result in far greater losses than employees' misappropriation of assets.

On compensation, market expectations and pressure to perform, the CPAB has this to say: “Auditors may learn that management has a strong incentive to manipulate financial results because a significant

Resserrer les contrôles

De nouveaux risques sont toujours émergents et « les méchants deviennent de jour en jour plus intelligents et raffinés », souligne l'administratrice Benita Warmbold, Fellow de l'Institut des administrateurs de sociétés et présidente du conseil d'administration du Conseil canadien sur la reddition de comptes, l'organisme réglementaire de surveillance des firmes vérificatrices des entreprises inscrites en bourse. Le CCRC est à élaborer de nouvelles normes afin de renforcer la qualité des audits reliés à la fraude et d'améliorer la capacité des auditeurs à identifier, évaluer et répondre aux risques de fraude.

La fraude existe, mais des cadres solides de contrôle interne peuvent en minimiser les risques. Idéalement, poursuit Mme Warmbold, « on veut d'abord empêcher le délit avant qu'il survienne. » Sinon, la capacité d'arriver rapidement à le stopper réduira au moins les dommages.

Dans le secteur des entreprises, des équipes d'audit externe ont incorporé des analyses de risque de fraude dans les inspections annuelles des rapports financiers de leurs clients. « Les administrateurs réalisent que la fraude peut avoir de sérieux impact sur leurs finances et leur réputation et, ultimement, sur les marchés d'investissement en général, » soutient Mme Warmbold, une comptable professionnelle agréée qui siège aussi aux conseils de la Banque Scotia, SNC Lavalin et Methanex Corp.

L'analyse thématique sur la fraude, publiée par le Conseil canadien de reddition de comptes en mai 2022, offre une indication de la surveillance approfondie à laquelle les organisations peuvent s'attendre sur les ententes de rémunération, l'efficacité des programmes de lanceurs d'alerte et la question de savoir si elles appliquent la lentille anti-fraude aussi rigoureusement aux membres de la direction qu'aux employés. Même si les organisations sont souvent réticentes à remettre en question l'intégrité de leurs gestionnaires, le CCRC souligne que les arnaques de rapports financiers frauduleux se traduisent par des pertes bien plus élevées que les malversations commises par les employés.

En ce qui concerne la rémunération, les attentes du marché et la

proportion of their compensation strategy (bonuses, stock options, etc.) is contingent on achieving aggressive financial targets Auditors may [also] learn that analysts have unduly aggressive or unrealistic expectations about an entity's financial performance by listening ... to earnings calls with analysts or reading [other] analysts' research reports."

If managers undertake to meet the analysts' "unrealistic expectations" on those earnings calls, the auditors are more likely to take a closer look at the books.

Board responsibility

While CPAB is working with the audit community, finance professor Alexander Dyck leads discussions about fraud in the ICD's Directors Education Program (DEP) at the University of Toronto's Rotman School of Management. It's always a galvanizing topic, says Dyck, who estimated in a recent research report that two-thirds of corporate frauds go undetected.

"The people best positioned to identify whether there is a problem are the directors because they can demand the information and take steps to correct it," says Dyck, an academic director of the DEP. In order to do this, though, directors need to think about "board composition issues on an ongoing basis to make sure they are best positioned to create and protect value."

They might also want to evaluate the independence of their external auditors, says Dyck, noting that – before the run on deposits and its recent demise – Silicon Valley Bank had used the same audit firm for more than 20 years. Does the audit firm's professional skepticism begin to fade after such a long tenure? Will the risk assessment be as rigorous?

"There is a lot of attention being paid to this in the U.S., there are a lot of shareholder proposals [suggesting that audit firms should be switched out after serving for a certain number of years.]"

To help directors better assess the likelihood of fraud taking place, Dyck and other researchers are delving into the financial statements of firms that had previously been caught.

"It's instructive to see the circumstances that lead to the likelihood of fraud, and one of them is the circumstance that we are seeing right now. The economy has been going well and then it starts to slow down and there are a lot of people who want to keep the music playing. There isn't very active monitoring because people have been doing well by the firm, so they give the benefit of the doubt to whatever is going on," says Dyck.

"This combination of high motive and low monitoring seems to be an active breeding ground for fraud" and misrepresentation in the financial reports, he says.

Corporate director Kenneth Hughes, a certified fraud examiner and former auditor-general for the City of Ottawa, says fraud risk assessments should capture both internal and external threats "when you look at all the other risks that you face, like ransomware and phishing expeditions to try to get someone to respond to an email that gives a bad actor access to your internal accounting, systems, for example."

The board's role is to ensure that management has conducted the fraud risk analysis, that it is updated regularly and that it is monitoring emerging risks. It cannot just be an annual exercise. "If you are monitoring emerging risks, you have to break the pattern, you

pression de produire, le CCRC a ceci à dire : « Les auditeurs peuvent apprendre que la direction a une forte motivation à manipuler les résultats financiers parce qu'une proportion importante de leur stratégie de rémunération repose sur l'atteinte de cibles financières dynamiques. (...) Les auditeurs peuvent aussi apprendre que les analystes ont adopté des attentes indûment agressives ou irréalistes quant à la performance financière de l'organisation en écoutant des entretiens avec des analystes ou en lisant les rapports de recherche de certains autres. »

Si les gestionnaires entreprennent d'adopter les « attentes irréalistes » des analystes exprimées lors de ces appels, les auditeurs sont plus susceptibles de regarder de plus près les rapports financiers.

Les responsabilités du conseil

Alors que le CCRC collabore avec la communauté d'audit, le professeur de finances Alexander Dyck mène des discussions sur la fraude dans le cadre du Programme de perfectionnement des administrateurs offert à la Rotman School of Management de l'Université de Toronto. Il s'agit toujours d'un sujet mobilisateur, explique M. Dyck, qui a estimé dans un rapport récent que les deux tiers des fraudes en entreprise demeurent non détectés.

« Les gens les mieux positionnés pour identifier s'il y a un problème sont les administrateurs parce qu'ils peuvent exiger l'information et prendre les mesures nécessaires pour corriger les choses », soutient M. Dyck. Pour y arriver, cependant, les administrateurs doivent songer aux « enjeux de composition du conseil de façon continue afin de s'assurer qu'ils sont les mieux en position de créer et protéger la valeur. »

Ils pourraient aussi vouloir évaluer l'indépendance de leurs auditeurs externes, poursuit-il, soulignant que la Banque Silicon Valley avait recouru à la même firme pendant plus de vingt ans. Est-ce que le scepticisme professionnel d'un cabinet d'audit commence à s'estomper après un tel mandat? L'évaluation du risque demeure-t-elle aussi rigoureuse?

Pour aider les administrateurs à mieux évaluer la probabilité d'une fraude en cours, le professeur Dyck et d'autres chercheurs approfondissent les rapports financiers des cabinets qui se sont récemment fait prendre.

« Il est instructif, poursuit-il, de voir les circonstances menant à la probabilité d'une fraude et l'une d'entre elles est celle dont nous sommes présentement témoins, explique M. Dyck. L'économie s'est bien comportée, puis elle a commencé à ralentir et il y a beaucoup de gens qui veulent que cette musique continue. La surveillance n'est pas très active parce que l'organisation est satisfaite de ses gens. Alors, elle leur donne le bénéfice du doute, peu importe ce qui se produit. »

« Cette combinaison de motivation élevée et de faible surveillance semble un terrain fertile pour la fraude, dit-il, et les fausses déclarations dans les rapports financiers. »

L'administrateur de sociétés Kenneth Hughes, un examinateur de fraude agréé et ancien vérificateur général de la Ville d'Ottawa, affirme que les évaluations de risque de fraude devraient englober à la fois les menaces internes et externes.

A stylized illustration in shades of blue and white. A large, blocky hand is shown holding a thick stack of dollar bills. The bills are white with a large blue dollar sign in the center. The background consists of jagged, mountain-like shapes in various shades of blue. The overall style is geometric and modern.

The combination of high motive and low monitoring creates a breeding ground for fraud, financial experts say.

Robust internal controls and a well-run whistleblower program can be a powerful deterrent to people who might otherwise commit fraud.

Des contrôles internes robustes et un programme de lanceur d'alerte bien mené peuvent s'avérer de puissants dissuasifs pour des gens qui autrement pourraient commettre une fraude.



can't stick to a schedule," says Hughes, a chartered professional accountant who chairs the board of Ottawa-based Your Credit Union Ltd. and serves on the board of Perley Health, an Ottawa-based not-for-profit organization that provides long-term care and independent living apartments for veterans and seniors.

Familiar patterns

Robust internal controls and a well-run whistleblower program can be a powerful deterrent to people who might otherwise commit fraud. Furthermore, the value of whistleblowers in alerting executives and boards to potential wrongdoing cannot be overstated, says Hughes. The Association of Certified Fraud Examiners reports that 42 per cent of occupational frauds are initially detected through tip lines. "Therefore, implementing effective processes to solicit and thoroughly evaluate tips is a crucial priority for fraud examiners," ACFE says in its report "Occupational Fraud 2022: A Report to the Nations." More than half of the tips come from employees and nearly one-third come from outside parties, including customers, vendors and competitors.

Whistleblower programs only have credibility if the tips are considered and acted on when necessary, says Hughes. CPAB says in its

Le rôle du conseil consiste à s'assurer que la direction ait mené une analyse du risque de fraude qui soient régulièrement mise à jour et surveille également les risques en émergence. Ça ne peut pas être qu'un exercice annuel. « Si vous surveillez des risques émergents, vous devez briser un modèle; vous ne pouvez pas vous en remettre seulement à un échéancier », souligne M. Hugues, un comptable professionnel agréé qui préside le conseil de Your Credit Union Ltd d'Ottawa et siège à celui de Perley Health, une organisation à but non lucratif qui offre des soins à long terme et des appartements à des anciens combattants et à des aînés.

Des modèles familiaux

Des contrôles internes robustes et un programme de lanceur d'alerte bien mené peuvent s'avérer de puissants dissuasifs pour des gens qui autrement pourraient commettre une fraude. En outre, on ne saurait trop souligner la valeur des lanceurs d'alerte qui préviennent la direction et les conseils de possibles méfaits. Plus de la moitié des indications à cet égard proviennent d'employés et près d'un tiers de tierces parties, dont des clients, des vendeurs et des concurrents.

Some of the biggest frauds Mak has seen have been perpetrated by high-level managers at smaller companies and family businesses.

Certaines des fraudes les plus massives dont M. Mak a été témoin ont été perpétrées par des cadres de haut niveau de petites entreprises et d'entreprises familiales.

fraud thematic review that the lack of a whistleblower program, or an ineffective one, may be indicative of weaknesses in the entity's control environment. External auditors are particularly interested in hearing from management or audit committee members about whether any of the tips received through this process relate to the entity's financial reporting. And, if so, how were they dealt with?

Directors should keep an open mind when issues raised by whistleblowers are elevated to the board level, says Warmbold. "You have to go at those with a high degree of skepticism – skepticism not being 'management is right and the whistleblower is wrong,' but really trying to think and be inquisitive as to what the whistleblower is getting at."

When a serious breach is raised with the board, directors should ask hard questions, says BDO's Mak. Some companies, reassured by management that "we have got it under control, it won't happen again, don't worry about it" don't probe any further. This is a mistake, Mak says. "As directors, it is important that we form our own understanding, a good understanding of what happened, how it happened, why it happened and [then] challenge management on why they don't think it would happen again."

Some of the biggest frauds Mak has seen have been perpetrated by high-level managers at smaller companies and family businesses, controllers and chief financial officers who have been in their positions for 10, 15 or 20-plus years. "They're trusted, they have gone to family weddings ... and they have perpetrated some of the biggest frauds because they have the ability, they have access to records, the signing authority, they can do it."

This fits with the Association of Certified Fraud Examiners research. "The ability to commit fraud is a skill, and our data suggests that the longer a person works for a company, the better they become at fraud," ACFE said in its report, which was based on 2,110 cases of occupational fraud in 133 countries investigated between January, 2020 and September, 2021.

Mak says the forensic specialists are typically called in after a potential fraud has been detected "and it hits the fan." CPAB is pushing audit teams to enlist their forensic colleagues earlier in the process to brainstorm on the factors they should take into account in order

Les programmes de lanceurs d'alerte ne seront toutefois crédibles que si ces indications sont prises en compte et font l'objet de mesures lorsque nécessaire. Le CCRC souligne dans son analyse thématique sur la fraude que le manque de programmes de lanceurs d'alerte – ou la présence d'un programme inefficace – peut révéler des faiblesses dans l'environnement de contrôle de l'organisation. Les auditeurs externes sont particulièrement intéressés à savoir de la part de la direction ou de membres du comité d'audit si l'une ou l'autre de ces indications est liée aux rapports financiers de l'organisation.

Les administrateurs devraient garder l'esprit ouvert quand des enjeux soulevés par des lanceurs d'alerte atteignent le niveau du conseil, explique Mme Warmbold. « Il faut aller vers ceux qui font preuve d'un degré élevé de scepticisme – le scepticisme n'étant pas l'idée que la direction a raison et que le lanceur d'alerte a tort, mais d'essayer vraiment de déterminer là où le lanceur d'alerte veut en venir. »

Quand une infraction grave est soulevée au conseil, les administrateurs devraient poser des questions difficiles, explique M. Mak. C'est une erreur que d'écouter la direction qui recommande de ne pas s'en faire et assure que ça ne se reproduira plus. « Comme administrateurs, il est important que nous formions notre propre compréhension de ce qui s'est produit, de la manière et des raisons pour lesquelles cela est arrivé. »

Certaines des fraudes les plus massives dont M. Mak a été témoin ont été perpétrées par des cadres de haut niveau de petites entreprises et d'entreprises familiales – contrôleurs et chefs de la direction financière qui ont été en poste pendant 10, 15 ou plus de 20 ans. « On leur fait confiance, ils ont assisté à plein de noces familiales (...) et ils ont perpétré certaines des fraudes les plus massives parce qu'ils en avaient la capacité, qu'ils avaient accès aux dossiers, à l'autorité de signature. »

« La capacité de commettre une fraude est un talent et nos données suggèrent que plus une personne travaille longtemps dans une entreprise, plus elle est susceptible de passer à l'acte », souligne l'Association des examinateurs agréés en fraude.

to perform a high-quality fraud risk identification and assessment.

This is welcome news to the forensics folks. "Focusing more on fraud risk analysis is as important as focusing on fraud that has actually occurred," says Hughes.

It makes sense to invite the accountants who specialize in financial crime investigation to share their expertise at the planning stage of an audit, says Mak. "It was always an informal practice, but it's becoming more common across the profession now, and that's an improvement." **DJ**

VIRGINIA GALT, a former business and education reporter for The Globe and Mail, covers legal, education and management issues for a number of publications.

M. Mak explique que les spécialistes juridiques sont généralement saisis du dossier après qu'une fraude possible ait été détectée et « dépasse les bornes. » C'est une bonne nouvelle pour ces spécialistes, soutient M. Hughes. « Se concentrer davantage sur l'analyse du risque de fraude est aussi important que de le faire sur des fraudes déjà survenues. »

Il serait logique d'inviter les comptables spécialisés dans les crimes financiers de partager leur expérience au stade de planification de l'audit, conclut M. Mak. **DJ**

VIRGINIA GALT, ex-journaliste spécialisée en économie et en éducation pour le Globe and Mail, couvre les questions juridiques, d'éducation et de gestion pour un certain nombre de publications.

CHEAT SHEET

How fraudsters steal, cover it up and get caught

Une fraude en entreprise dure en général 12 mois avant d'être détectée

No organization is immune from fraudsters, says the Association of Certified Fraud Examiners in its international study "Occupational Fraud 2022: A Report to the Nations." They attack large multinational businesses, small private companies, government agencies and non-profits. The report is based on 2,100 cases of occupational fraud investigated between January, 2020 and September, 2021 in 133 countries.

THE FINANCIAL TOLL

Financial statement fraud accounted for only 9 per cent of cases, but was the most damaging, with a median loss of US\$593,000 per case, says the ACFE, noting that fraudsters do not necessarily limit themselves to one form of fraud.

Corruption (including bribery, conflicts of interest and extortion) was found in 50 per cent of the cases, with a median loss of US\$150,000.

Asset misallocation (including theft, false billing schemes and inflated expense reports) was found in 89 per cent of the cases, causing a median loss of US\$100,000.

THE COVER UP

The top five concealment methods reported by the ACFE are: creation of fraudulent physical documents, alteration of physical documents, creation of false electronic documents, alteration of electronic documents, and destruction or withholding of physical documents.

BUSTED

The old-fashioned whistleblower line is the most effective method for detecting fraud, accounting for 42 per cent of investigations. Most tips come from employees. Internal audits catch 16 per cent, and management reviews detect 12 per cent, the ACFE reports.

CRYPTO CRIME

Eight per cent of cases in the study involved cryptocurrency, most frequently used for bribes, kickbacks and converting misappropriated assets. "Anecdotal evidence suggests this number will rise in future years," the ACFE says in its report.

Aucune organisation n'est à l'abri des fraudeurs, affirme l'Association des inspecteurs certifiés de fraudes dans son étude internationale « Occupational Fraud 2022 : A Report to the Nations ». Les fraudeurs s'attaquent aux grandes entreprises multinationales, aux petites entreprises privées, aux agences gouvernementales et aux organisations à but non lucratif. Ce rapport est fondé sur quelque 2 100 cas de fraude en entreprise qui ont fait l'objet d'enquêtes entre janvier 2020 et septembre 2021 dans 133 pays.

LE COÛT ÉCONOMIQUE

Les fraudes associées aux rapports financiers n'ont compté que pour 9 pour cent des cas, mais les plus accablants, avec une perte médiane de 593 000 dollars US par cas, montrent que les fraudeurs ne se limitent pas nécessairement à une seule forme de fraude.

La corruption (dont les pots-de-vin, les conflits d'intérêts et l'extorsion) a été utilisée dans 50 pour cent des cas, pour une perte médiane de 150 000 dollars US.

La mauvaise allocation de ressources (vol, fausse facturation et notes de frais gonflées) a été utilisée dans 89 pour cent des cas, causant une perte médiane de 100 000 dollars US.

LA DISSIMULATION

Les cinq principales méthodes de dissimulation rapportées par l'AICF sont la création de documents physiques frauduleux, l'altération de documents physiques, la création de faux documents électroniques, l'altération de documents électroniques ainsi que la destruction ou la retenue de documents physiques.

CRYPTO CRIME

Huit pour cent des cas impliquent de la cryptomonnaie, des pots-de-vin et la conversion de ressources détournée. « Tout indique que ces façons de faire augmenteront dans l'avenir », signale l'AICF dans son rapport.

- VG