Grant Thornton

An instinct for growth™

# Conhecimento é poder: Proteja sua empresa promovendo *awareness* do risco de fraude

Toda empresa, de qualquer tamanho ou segmento, pode ser vítima de um ato ilícito. Na realidade, de acordo com a ACFE (*Association of Certified Fraud Examiners*), todo ano uma empresa perde cerca de 5% de seu faturamento em fraudes — totalizando uma perda média de USD $130,000 por transação fraudulenta. Esse tipo de atividade criminosa impacta não somente a rentabilidade dos negócios, mas também afeta drasticamente sua cultura, reputação e continuidade dos negócios.

Felizmente, muita coisa pode ser feita para proteger sua empresa de atividades ilícitas — a primeira delas pode ser aumentar o *awareness* do risco de fraude em sua organização. Na Grant Thornton, trabalhamos junto às empresas de todos os tamanhos, nas mais diversas indústrias, para ajudá-las a identificar – e mitigar – riscos de fraude que impactam o seu negócio.

## Um olhar mais atento

Como o único limite do fraudador é a imaginação, é impossível proteger sua empresa de todos os tipos de atividades fraudulentas ou prever precisamente que forma a tipologia de fraude tomará no futuro. Elevar o nível de *awareness* de fraude dentro da organização pode ajudá-la a identificar comportamentos arriscados. De maneira geral, é preciso conhecer as frentes internas e externas, uma vez que os negócios estão sujeitos à ação de fraudadores de fora e de dentro da organização. Abaixo, exploramos tendências e cenários de fraude comuns que podem ocorrer tanto interna como externamente.

## Fontes externas

**Fraudes virtuais**

Embora existam inúmeras modalidades de fraudes externas, atualmente, a mais comum é a fraude virtual, que, de acordo com o "*Canadian Anti-Fraud Centre*" (CAFC), significa "qualquer atividade falsa, enganosa, deturpada ou fraudulenta praticada contra vítimas potenciais que utilizam a internet."[2]

***Ransomware*:** Também chamado "*cyber* extorsão", o *ransomware* penetra nos sistemas de computadores das empresas e criptografa os dados das empresas. Os fraudadores exigem que a empresa afetada pague um resgate para liberar os sistemas. Às vezes, os criminosos ameaçam tornar públicos os dados caso a empresa se recuse a fazer o pagamento.

**Furto de dados:** Além de furtar dinheiro em espécie, dados também são alvo dos fraudadores. Esses dados podem incluir:

1. informações financeiras que eles possam usar para cometer fraude secundária;
2. dados proprietários que eles possam vender para a concorrência;
3. informações confidenciais pessoais (p.ex. prontuários médicos, números de seguridade social de seus clientes ou funcionários, contas financeiras, senhas) que eles consigam vender na *deep web* para ladrões de identidades.

***Banking* malware:** Esse tipo de fraude ocorre quando *cyber*-criminosos sofisticados têm como alvo usuários de *internet banking* — basicamente sequestrando a conexão entre o usuário de *internet banking* e o banco. Ao acessar o site do banco, o usuário se depara com uma tela que simula a página do portal, quando, na realidade, trata-se de uma réplica manipulada por criminosos — permitindo a eles roubar senhas e informações.

***Business email compromise* (BEC):** É um tipo de golpe em que o criminoso envia e-mails, geralmente fazendo-se passar pelo CEO, CFO ou outro funcionário do alto escalão da empresa. Os relatórios do FBI apontam que esse tipo de golpe causou às empresas prejuízos superiores a $1 bilhão em 2016.[3] Utilizando um e-mail falso — mas bastante convincente — os criminosos pedem que o destinatário do e-mail efetue um pagamento urgente. Mais recentemente, começaram inclusive a informar que as informações bancárias de um determinado fornecedor mudaram — e, em seguida, fornecem detalhes de sua própria conta. Quando o próximo pagamento é efetuado, o dinheiro vai para os criminosos, e não para o fornecedor.

**ATENÇÃO:**
Se você receber uma solicitação por e-mail, incluindo instruções para efetuar pagamentos, certifique-se de que os detalhes sejam verificados de maneira independente. Instruções via e-mail não são legítimas o suficiente para suportar pagamentos, efetuar processamento e proteger sua empresa de fraudes.

**ATENÇÃO:**
Se um fornecedor lhe pedir para alterar suas informações de pagamento e você notar um aumento nos pedidos de mudança; ou se fornecedores que você não reconhece estiverem apresentando faturas, verifique a atividade com a empresa — por telefone ou pessoalmente — o mais rápido possível. Reveja seus controles internos e processos de pagamento regularmente e verifique se eles efetivamente protegem seu negócio e permitem que você confirme ou receba de seus fornecedores os valores acordados.

Há uma série de ações que podem ser tomadas para proteger sua empresa da fraude virtual:

1. **Instalar e manter um *software* antimalware robusto.** Embora não seja 100% eficaz, os *softwares* devem detectar ao menos um número razoável de ameaças.
2. **Promover o *awareness* do risco de fraude.** Todos na empresa devem ser capazes de identificar os tipos mais comuns de fraude virtual — como, por exemplo, phishing, links chamativos (iscas), e BEC — e proteger informações pessoais que compartilham nas redes sociais.
3. **Proteger tudo com senha.** Servidores, VPNs, e-mails, roteadores— tudo o que se conectar com a internet — devem ser protegidos com uma senha segura, não com a senha padrão que vem com o produto quando adquirido.
4. **Atualizar *softwares*.** Verifique se o sistema está configurado para instalar todas as atualizações críticas, quando disponíveis.
5. **Proteger dados críticos.** Identifique quais dados são críticos para sua organização — como, por exemplo, dados financeiros, informações pessoais e informações do cliente — e proteja-os.
6. **Fazer *backups*.** A melhor proteção contra *ransomware* é um programa de *backup* confiável, que não possa ser facilmente acessado através dos sistemas utilizados no dia a dia.

Vale ressaltar que os fraudadores externos não se restringem à internet. Seguem exemplos de outros tipos de ameaças externas às quais sua empresa precisar estar atenta:

**Parceria de negócios:** Parceria de negócios: Ao estabelecer um negócio internacional, muitas empresas optam por fazer parcerias de negócios com prestadores de serviços. Reconhecendo isso, os criminosos começaram a personificar empresas legítimas — como agentes de cobrança — e usando sua posição para acessar informações e defraudar seus "clientes". Proteja-se realizando uma diligência (isto é, verifique os antecedentes) da entidade e das pessoas.

**Falso fornecedor:** Sem uma diligência preventiva e constante, muitas empresas são vítimas da fraude do falso fornecedor — que pode incluir superfaturamento, faturamento de trabalhos incompletos, fixação de preços, faturas em duplicidade, ou substituição de produtos. Em certos casos, os fraudadores tentarão se passar por um fornecedor real — talvez criando um nome parecido com o de um fornecedor legítimo e reconhecido — e emitindo faturas falsas para desviar recursos.

**Licitação fraudulenta:** Esse tipo de fraude envolve violação do processo de licitação que as empresas realizam para selecionar e homologar relacionamentos com fornecedores. Nesse tipo de fraude, dois fornecedores entram em conluio; um dos fornecedores faz uma oferta menos atraente para garantir que o outro vença o processo de licitação. Os papéis se invertem no projeto seguinte.

## Golpes contra pessoas físicas também existem

O número de fraudes contra corporações está crescendo, mas as empresas não são os únicos alvos. Pessoas físicas—inclusive empresários e administradores—costumam ser vítimas de diversos esquemas de fraude, entre os quais:

**Passar-se por agente da Receita Federal:** Desde janeiro de 2014, os canadenses pagaram mais de $6,2 milhões[4] a fraudadores internacionais que fingem ser agentes da Receita Federal do Canadá (CRA) à procura de dívidas fiscais em aberto ou se oferecendo para resolver assuntos financeiros relacionados com imigração.

**Falso investimento:** Se uma oportunidade de investimento parece boa demais para ser verdade, desconfie. Esse tipo de fraude geralmente apresenta uma oportunidade de ganhar dinheiro rápido, mas não oferece muitos detalhes e exige que você tome decisões rapidamente. Qualquer coisa pode ser objeto desse tipo de fraude, desde um processo de ICO (Oferta Inicial de Moeda), que promete altos retornos sobre investimentos em *Bitcoin*, ou o esquema Ponzi, que promete pagar rendimentos astronômicos a seus investidores usando o dinheiro das vítimas que chegaram depois para pagar as vítimas que chegaram antes, numa tentativa de manter o esquema funcionando

## Fontes internas

Internamente, o *awareness* também precisa ser alto. "Fraude ocupacional" é a fraude cometida dentro de uma organização — ou por seus administradores, diretores ou funcionários. De acordo com a ACFE, a fraude ocupacional pode ser dividida em três grandes categorias: apropriação indébita de ativos, corrupção e fraude nas demonstrações financeiras.

### Apropriação indébita de ativos:

A apropriação indébita de ativos responde por 89% das fraudes internas que vêm sendo relatadas[5] e ocorre quando os responsáveis por processos ou gerenciamento dos ativos de valor da organização, optam por furtá-los. Nesse contexto, ativos significam desde dinheiro até estoques.

A apropriação indébita de ativos geralmente consiste em furto, por parte do funcionário ou do administrador, do fundo de caixa ou de recebimentos em dinheiro sem documentação interna, mas também pode incluir outros esquemas. Por exemplo, alguém pode criar um funcionário fantasma, adicioná-lo à folha de pagamento e embolsar o salário do novo funcionário. Ou então, um administrador pode cadastrar um fornecedor fantasma no sistema – e receber milhares de dólares se a empresa pagar o fornecedor sem confirmar sua existência ou se não houver controles sobre o processamento de pagamentos. A apropriação indébita de estoques pode ocorrer quando uma pessoa do departamento responsável pelo recebimento e embarque de mercadorias deixa de registrar um item quando este dá entrada na empresa – e opta por furtá-lo. Em muitos casos, a empresa simplesmente assume que o item extraviou durante o trânsito.

**Corrupção:** Corrupção é um termo amplamente utilizado para designar diferentes tipos de fraudes. Refere-se mais comumente a funcionários ou administradores que fazem alianças pessoais com partes externas e coloca esses relacionamentos acima dos interesses da empresa. Esse tipo de fraude ocorre em 38% dos casos de fraudes corporativas, de acordo com o ACFE, e causa às empresas um prejuízo médio de USD $250,000.6 Corrupção pode englobar desde conflitos de interesse (p.e., esquemas de compra e venda); gratificações ilícitas; até subornos, como, por exemplo, propinas. Ocorre suborno quando um fornecedor oferece ao funcionário ou administrador um incentivo pessoal em troca de um benefício específico. O incentivo pode ser na forma de recursos financeiros — por exemplo, um percentual sobre o valor total de um projeto — ou na forma de um serviço ou outro benefício pessoal.

Um código de conduta transparente deve fornecer diretrizes claras aos funcionários. É permitido aceitar ingressos para eventos esportivos de um fornecedor? Se sim, até que valor? E se o evento for acontecer em outra cidade e todos os custos da viagem também estiverem sendo cobertos? As respostas a essas perguntas irão depender da sua empresa, da natureza dos relacionamentos e do quanto a empresa está disposta a permitir.

**ATENÇÃO:**
**Se um funcionário ou administrador nunca tira férias, intimida outros funcionários, aparenta estar vivendo além de seus meios e/ou aparenta estar passando por uma mudança de estilo de vida radical, é possível que a pessoa esteja em grande dificuldade financeira, e os níveis de *awareness* de fraude devem se elevar.**

**ATENÇÃO:**
Verifique se um funcionário ou administrador parece ter um relacionamento próximo demais com um determinado fornecedor — por exemplo, fazendo viagens integralmente bancadas pelo fornecedor.

**Fraude das demonstrações financeiras:** Superavaliar o patrimônio líquido/lucro líquido de uma organização geralmente envolve falsificar registros relacionados com receitas, passivos, despesas e avaliação de ativos. Várias são as motivações para esse tipo de fraude, porém a mais frequente é obter ganho pessoal—por exemplo, inflar o desempenho operacional para receber um bônus mais alto, fazer a organização parecer melhor do que está aos olhos dos investidores ou credores, ou acobertar outros tipos de fraude/risco.

Há uma série de ações que podem ser tomadas para proteger sua empresa de fraude interna:

1. **Implantar um canal de denúncias.** De acordo com o ACFE 40% das fraudes são descobertas através de relatos — e, desses relatos, 53% partem dos funcionários ou outras pessoas de dentro da empresa. Um canal de denúncias gerenciado adequadamente — e bem promovido — é uma maneira eficaz e econômica de estimular relatos de fraude e reduzir o tempo que levaria para identificar incidências de fraude ocupacional.

2. **Realizar uma avaliação do risco de fraude.** A avaliação do risco de fraude pode ser um exercício minucioso, detalhado – mas não precisa ser. Uma abordagem em fases, com passos iniciais, é capaz de apoiar e elevar consideravelmente o nível de *awareness* de fraude entre as pessoas da empresa, além de ajudar a proteger o futuro da organização.

3. **Promover treinamentos que elevem o *awareness* do risco de fraude.** Uma vez que os funcionários tenham um canal para relatar comportamento fraudulento, é importante educá-los sobre como alavancar esse canal. A ideia é que seus funcionários se tornem seus "olhos e ouvidos". Não é possível fazer isso sozinho.

4. **Implantar e divulgar um código de conduta. Estabelecer o tom da administração.** Para criar uma organização consciente do risco de fraude, o *awareness* deve estar embutido em sua cultura. Isso exigirá o engajamento da alta administração — e a implantação de um código de conduta claro e bem divulgado.

5. **Implementar checagens e travas.** Segregar funções e controlar o acesso a informações sensíveis, estoques, caixa e outros ativos, protegendo-os com senha ou com algum outro método, são medidas que dificultam atitudes fraudulentas que estejam no radar.

## Entenda o risco de fraude no contexto de sua empresa

Tanto interna como externamente, as empresas estão sujeitas a fraudes. Por isso é tão importante não adiar ações que protejam sua empresa, seus funcionários e sua reputação. Nossa vasta experiência demonstra que elevar o nível de *awareness* do risco de fraude efetivamente tem um impacto tremendo.

Para defender seus negócios do risco de fraude, primeiro é necessário saber quais são as vulnerabilidades. Uma avaliação do risco de fraude pode ajudar a empresa a entender os riscos prevalentes no mercado, os ativos mais vulneráveis e o estágio atual de seus processos e controles, além de ajudar a identificar *gaps* e estabelecer um plano para fortalecer seus controles antifraude. Isto poderia incluir qualquer ação, desde implantar um treinamento mais robusto até investir em um seguro contra fraude.

## Saiba como responder — e se recuperar

Se o impensável acontecer, sua empresa pode ser pega desprevenida. Ter uma resposta e um plano de gestão de crise pode não só encurtar a duração do comportamento fraudulento e trazer economias ao processo, mas ajudar sua empresa a se recuperar mais rapidamente. Saber como preservar a evidência de uma fraude também pode dar aos investigadores uma excelente oportunidade de pegar fraudadores, além de fortalecer as defesas da empresa, para evitar que a história se repita.

1 Association of Certified Fraud Examiners. 2018. "Report to the Nations: 2018 Global Study on Occupational Fraud and Abuse". Page 4. https://s3-us-west-2.amazonaws.com/acfepublic/2018-report-to-the-nations.pdf
2 Canadian Anti-Fraud Centre. April 27, 2017. "Fraud Types". Government of Canada. http://www.antifraudcentre-centreantifraude.ca/fraud-escroquerie/index-eng.htm
3 Better Business Bureau. November 9, 2017. "FBI Says Business Email Compromise Scams Continue to Grow in U.S., Cost Companies More Than $1 Billion". https://www.bbb.org/stlouis/news-events/news-releases/2017/11/cftf-bec/
4 Hermann, Penny. January 23, 2017. "CRA scam continues, but with a new twist". Royal Canadian Mounted Police. http://www.rcmp-grc.gc.ca/en/news/2017/23/cra-scam-continues-a-new-twist
5 Association of Certified Fraud Examiners. 2018. "Report to the Nations: 2018 Global Study on Occupational Fraud and Abuse". Page 4. https://s3-us-west-2.amazonaws.com/acfepublic/2018-report-to-the-nations.pdf
6 Association of Certified Fraud Examiners. 2018. "Report to the Nations: 2018 Global Study on Occupational Fraud and Abuse". Page 10. https://s3-us-west-2.amazonaws.com/acfepublic/2018-report-to-the-nations.pdf
7 Association of Certified Fraud Examiners. 2018. "Report to the Nations: 2018 Global Study on Occupational Fraud and Abuse". Page 4. https://s3-us-west-2.amazonaws.com/acfepublic/2018-report-to-the-nations.pdf

**Para saber mais sobre como a Grant Thornton pode ajudar sua organização a se proteger, entre em contato com as nossas equipes:**

## Brasil


**Vitor Pedrozo**
Partner
**M** +55 11 97563-1778
**E** vitor.pedrozo@br.gt.com

**Aryadne Mello**
Gerente
**M** +55 11 99188-7138
**E** aryadne.mello@br.gt.com

**Joao Moretto**
Gerente
**M** +55 11 95628-6129
**E** joao.moretto@br.gt.com

**Delson Goncalves**
Gerente
**M** +55 11 97777-1090
**E** delson.goncalves@br.gt.com

**Rodrigo Akamine**
Gerente
**M** +55 11 97378-7247
**E** rodrigo.akamine@br.gt.com

**Claudio Castro**
Gerente
**M** +55 11 98995-6464
**E** claudio.castro@br.gt.com


## Canada


**Jennifer Fiddian-Green**
Partner, National Forensics and Dispute Services Leader
**T** +1 416 360 495 7957
**E** Jennifer.Fiddian-Green@ca.gt.com

**Leah White**
Partner
**T** +1 902 491 7718
**E** Leah.White@ca.gt.com

**Jeff Merrick**
Senior Manager
**T** +1 902 420 7197
**E** Jeff.Merrick@ca.gt.com

**Adam Lippa**
Senior Manager
**T** +1 709 778 8842
**E** Adam.Lippa@ca.gt.com

**David Malamed**
Partner
**T** +1 416 360 3382
**E** David.Malamed@ca.gt.com

**David Florio**
Partner
**T** +1 416 369 6415
**E** David.Florio@ca.gt.com

**Sandy Boucher**
Senior Manager
**T** + 1 416 369 7027
**E** Sandy.Boucher@ca.gt.com

**Eric Au**
Senior Manager
**T** + 1 416 369 7069
**E** Eric.Au@ca.gt.com

**Mohamed Elghazouly**
Senior Manager
**T** +1 416 607 8762
**E** Mohamed.Elghazouly@ca.gt.com

**Ali Jaffer**
Senior Manager
**T** +1 416 607 2612
**E** Ali.Jaffer@ca.gt.com

**Dwayne King**
Senior Manager
**T** +1 416 607 8717
**E** Dwayne.King@ca.gt.com

**Robert Osbourne**
Senior Manager
**T** +1 416 360 4988
**E** Robert.Osbourne@ca.gt.com

**Jennifer Pavlov**
Senior Manager
**T** +1 416 369 6421
**E** Jen.Pavlov@ca.gt.com

**Shane Troyer**
Partner
**T**+1 604 443 2148
**E** Shane.Troyer@ca.gt.com

**Caroline Hillyard**
Senior Manager
**T** +1 604 697 7941
**E** Caroline.Hillyard@ca.gt.com

**Mohammad Pahrbod**
Senior Manager
**T** +1 604 687 2711
**E** Mohammad.Pahrbod@ca.gt.com


Grant Thornton
An instinct for growth™

**grantthornton.ca**



**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. We help dynamic organizations unlock their potential for growth by providing meaningful, actionable advice through a broad range of services. Together with the Quebec firm Raymond Chabot Grant Thornton LLP, Grant Thornton in Canada has approximately 4,000 people in offices across Canada.
Grant Thornton LLP is a Canadian member of Grant Thornton International Ltd, whose member firms operate in over 130 countries worldwide.