



## Be On The Lookout For Occupational Fraud

🔒 risk management fraud protection employees

**Summary:** Occupational fraud is the biggest threat facing small businesses. What you and your business customers should know.

Yet another Bank Director survey of board members and management finds 72% of banks surveyed said they had not experienced a data breach or cyberattack, but 62% said their board did not have at least one cybersecurity expert member and only 49% said they had a full-time chief information security officer (CISO). Banks are working on this, but given the move towards more fintech and banktech, this is one area we would expect to see a growing emphasis with all banks going forward.

There has been no shortage of attention paid to the rising volume of cybercrime and its impact on both consumers and businesses. It is a tall order to minimize cybercrime, but for small businesses, it turns out that one of the biggest threats they face is actually within their own organizations - occupational fraud.

Occupational fraud is defined as, "the use of one's occupation for personal enrichment." According to the Association of Certified Fraud Examiners (ACFE), small businesses have more than their fair share of this issue.

In its [2018 Report to the Nations](#), the ACFE's biennial study found the largest amount of internal fraud occurs within businesses that have fewer than 100 employees, with 28% of such fraud cases. Further, businesses within this group faced the greatest median loss at \$200k, which can be particularly damaging since such businesses often don't have the resources necessary to recover from losses incurred.

Unfortunately, it is not uncommon for employees who have been given a great deal of trust by their employers to take advantage of their positions for their own gain, by misusing the organization's assets or resources. In fact, theft of assets is the most frequent and costliest form of fraud experienced by small companies, followed by corruption schemes and finally financial statement fraud. In many cases, the fraud experienced by smaller companies involves a combination of the above.

Most fraud is not just a one off, as the median length of time that it goes on before being discovered is 16 months. Needless to say, the longer fraud goes on, the more costly and damaging it ultimately proves to be.

When it comes to the ways that fraud is typically discovered, tips generated by individuals inside and outside the company come in on top (40%) followed by an internal or external audit (19%) followed by management review (13%). Given this reality, community banks would be well served to encourage employees, as well as customers and vendors, to report any instances of fraud they suspect or see. The best way of doing this is by allowing people to anonymously report such instances, so there is no fear of retaliation from the employees that they turn in.

Of course, the best thing to do is to stop fraud in the first place. Steps to take include: avoid giving any one employee too much responsibility and provide adequate oversight--all of which should be outlined in written policies; divide up tasks among multiple employees; make sure to have proper documentation, along with the regular review of financial reports; and don't give employees more access or authority than their position necessitates.

Knowing all of this, encourage your customers to think not only as a small business owner, but also as a prudent risk manager, to help protect them and you.

## CHECK IMAGING FOR CANADIAN CASH LETTERS

PCBB's enhanced cash letter service for Canadian checks can help your bank minimize its credit exposure, increase operational efficiency and deliver faster fraud notification. Learn more about our [check imaging for Canadian cash letters](#).

*Copyright 2021 PCBB. Information contained herein is based on sources we believe to be reliable, but its accuracy is not guaranteed. Customers should rely on their own outside counsel or accounting firm to address specific circumstances. This document cannot be reproduced or redistributed outside of your institution without the written consent of PCBB.*