6 Tips to Help Small to Mid-Sized Businesses Combat Fraud

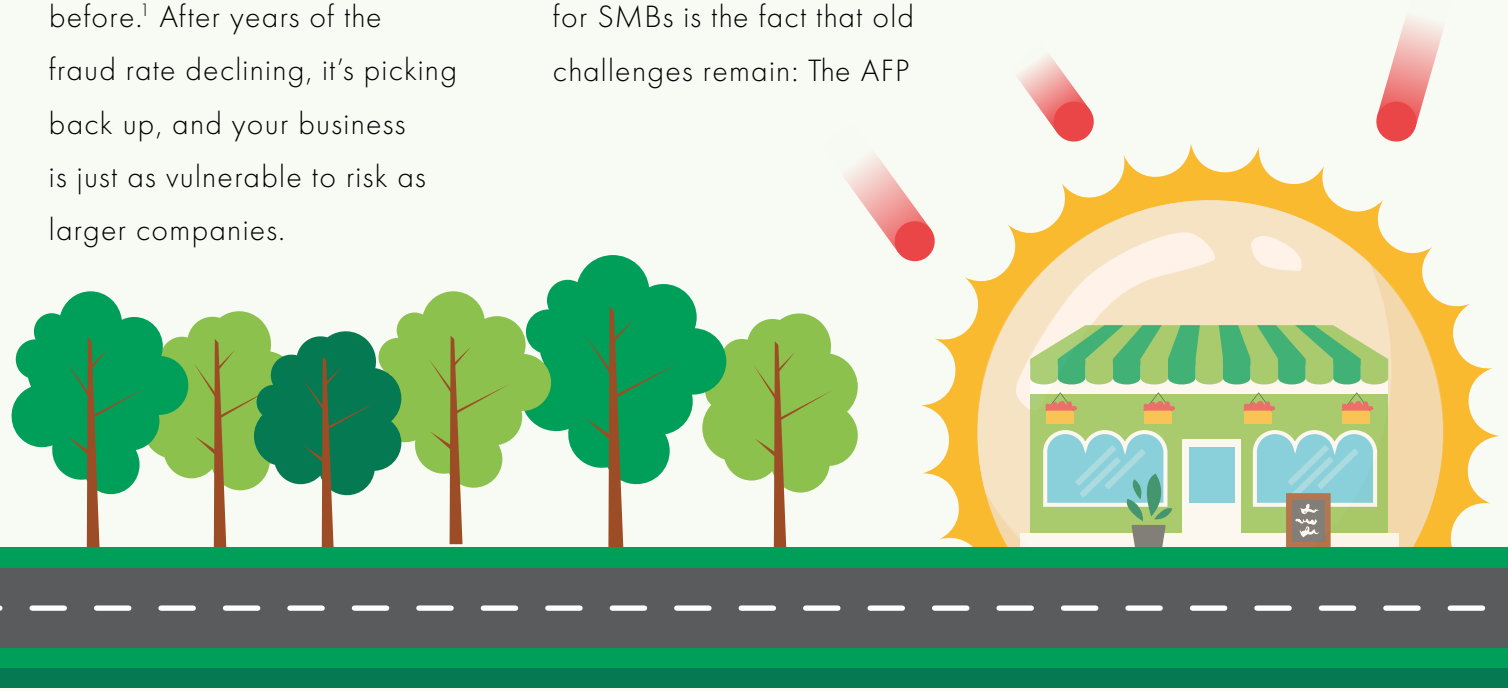
Central Bank

Contents

Introduction

With the digital transformation of culture and business, new openings for fraudsters have quickly emerged. According to a survey conducted by the Association for Financial Professionals (AFP), 74 percent of all businesses experienced an instance of fraud the year before.[1] After years of the fraud rate declining, it's picking back up, and your business is just as vulnerable to risk as larger companies.

The online threat landscape has evolved to a point where advanced techniques like ransomware consistently target small to mid-sized businesses (SMBs), who must also guard against other means like phishing and data attacks. Complicating the situation for SMBs is the fact that old challenges remain: The AFP survey also found 75 percent experienced **check fraud**. More than ever, business owners need information on **types of fraud** and ways to combat them. Check out these strategies you can use to protect your businesses and your customers.



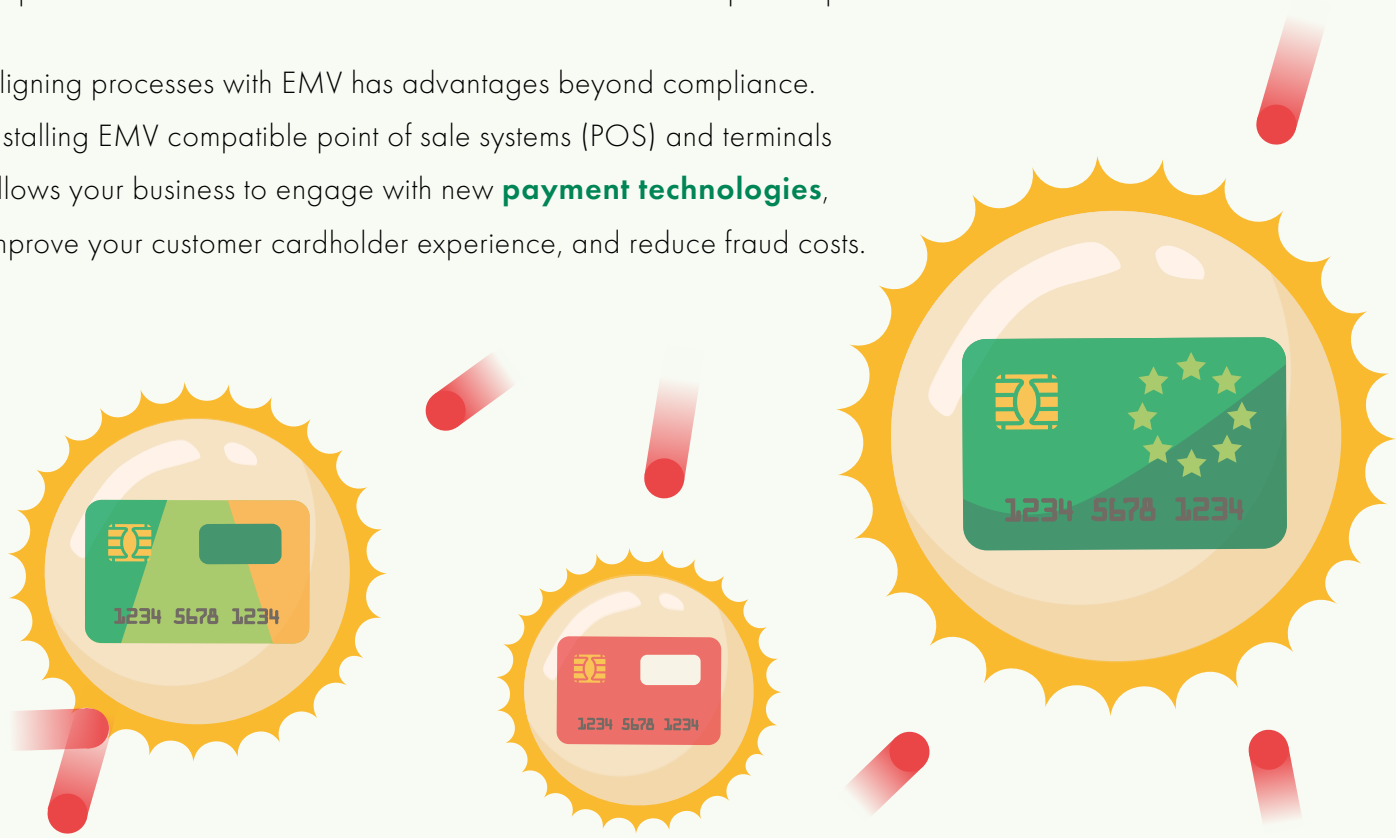
[1]https://www.afponline.org/publications-data-tools/reports/survey-research-economic-data/Details/payments-fraud-2016/

Tip #1 Become EMV-Compliant

Counterfeit card fraud is a particularly costly and frequent threat businesses have to deal with. That's why **EMV technology** was introduced, which replaced a card's information-holding magnetic stripe with a chip.

If you've been waiting to implement this change, you will want to get on board, and soon. A change to EMV standards has shifted liability for fraudulent transactions to merchants, meaning your business will be responsible for at least some of the costs of fraudulent in-person purchases.

Aligning processes with EMV has advantages beyond compliance. Installing EMV compatible point of sale systems (POS) and terminals allows your business to engage with new **payment technologies**, improve your customer cardholder experience, and reduce fraud costs.



Tip #2 Focus on ACH Protections

Transactions process with lightning-quick speed nowadays, and many consumers expect such immediacy. While mobile payment adoption is increasing, you might also utilize the **automated clearing house** (commonly referred to as ACH), the electronic network that really started it all, and which is used for direct deposit and debit transfers.

Security measures need to be top of mind for SMBs, even with ACH. The AFP survey found that ACH fraud was reported at 30 percent of organizations surveyed in 2016 (making it the fourth-most frequent), an increase of 5 percent from the year before, the largest uptick among fraud types.

The main way SMBs can tackle ACH fraud is by installing blocks and filters on transactions. These steps - which allow users to block unauthorized debits and filter genuine charges - can help SMBs manage an increasingly popular type of fraud.

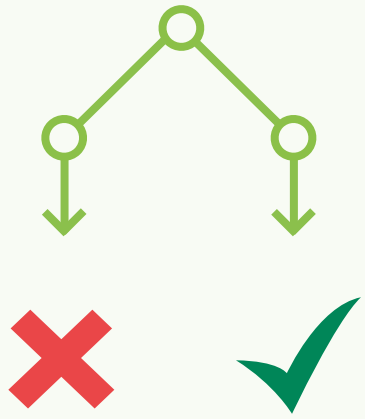
Tip #3 Don't Forget About Check Fraud

Even as digital pay methods continue to grab the spotlight, check fraud remains the No. 1 most likely type of scam to be experienced by an SMB. Organizations, in essence, need to fight a two-front war, one against both physical and digital forms of fraud.

Some of the most-used forms of protection against check fraud, according to AFP, include:

- Positive Pay (74 percent)
- Account segregation (69 percent)
- Daily reconciliation and internal processes (64 percent)

Positive Pay is an especially important safeguard for SMBs to have to avoid fraud costs. Positive Pay matches the dollar amount, check number and account number with all previously issued checks, simplifying and securing account reconciliation.

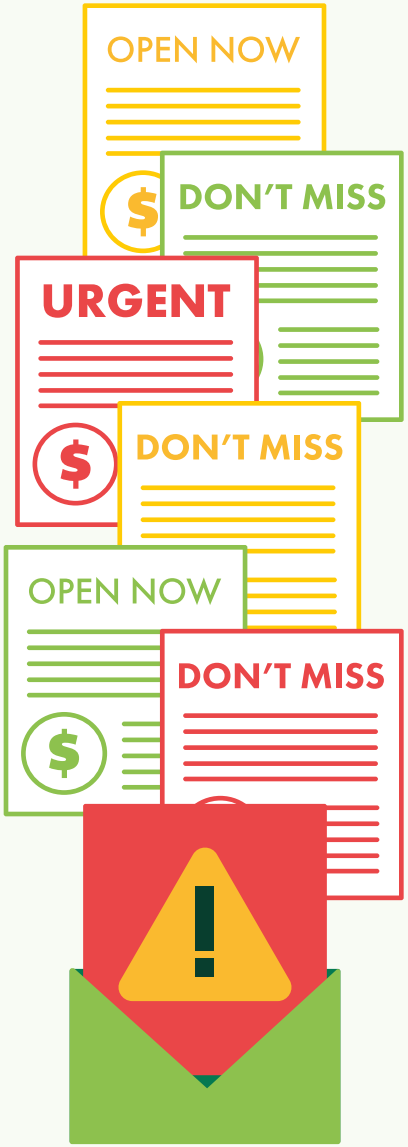


Though only 10 percent of respondents said they experienced check fraud-related financial loss, of that number, 23 percent cited lack of Positive Pay as the main reason for losses.

Tip #4 Train Employees to Spot the Signs

In the battle against fraud, most all SMBs' frontline defenses are made of the employees who process and handle transactions. Business leaders must then ensure they've educated employees on how and why fraud occurs, as well as empower them with the tools and skills to raise alerts or take action when needed.[2]

One particular point to stress with employees is **email phishing**. According to AFP, the second-most common source of fraud was email designed to compromise the business (reported by 54 percent of organizations).



Some of the indicators of an email with malevolent intentions include:

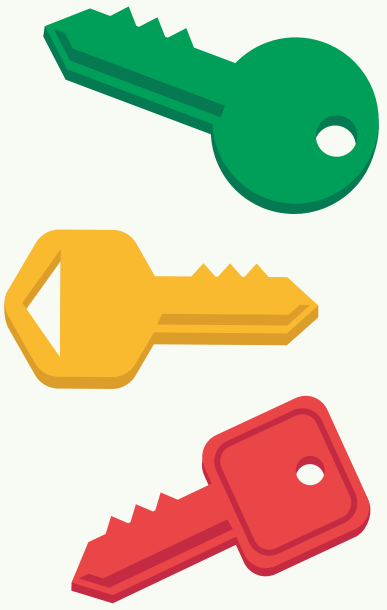
- Scrutinizing emails from even known names and addresses with suspicious subjects.
- Subject lines that include "URGENT," "OPEN NOW" or "DO NOT MISS!"
- The instruction to download or a view an attachment that you are not expecting or are not sure is 100 percent safe.

[2]https://blog.netwrix.com/2017/06/09/infographics-top-cybersecurity-risks-2017/

Tip #5 Be Smart About Cyberdefenses

As more SMBs engage with solutions like the cloud and mobile applications, the risk of a **cyberattack** grows as well. According to a recent Newtrix survey, just one-quarter of small and medium-sized businesses feel they are well-prepared for a data breach or other cybercrime-related event.[3]

You may think that you can forgo robust **cyberdefenses**, but hackers do not constrain their focus to solely multinational companies. A recent Datto survey found SMBs paid out $301 million to ransomware attackers to unencrypt data; 99 percent surveyed expected such attacks to rise.[4]



Ensure you have adequate tools to combat cyberattacks by focusing on steps like:

- Mobile and online banking sign-in processes that require two-part authentication (like combining PIN and fingerprint)
- Sufficient encryption of sensitive or personally identifiable customer data

[3]https://blog.netwrix.com/2017/06/09/infographics-top-cybersecurity-risks-2017/
[4]https://www.datto.com/news/datto-releases-global-state-of-the-channel-ransomware-report

Tip #6 Work With a Banking Partner That has Solutions

In the end, although you may do all in your power to **raise protections against fraud** and educate employees, you may not be able to completely protect your business all on your own. That's why companies need to have a partner in ensuring their assets are guarded, their data is safe, and that measures are in place to combat fraud.

Central Bank takes such responsibilities seriously and offers a range of fraud protection services SMBs can take advantage of, including:

- EMV-enabled point-of-sale terminals.
- ACH Blocks and Filters.
- Check fraud detection with Positive Pay and Payee Positive Pay.
- Re$ubmitIt® - a program to ensure you collect 100 percent of bad checks.

Conclusion

As a business owner, you must be ever vigilant in protecting yourself against fraud. The task is a particularly difficult one, considering all the angles from which fraud may attack. That is why you must take precise steps to build your defenses on both the frontline and cyber level of your business.

This includes not only implementing tools, but also offering training for employees on spotting signs of fraud or setting a standard for your own devised best practices.

When looking for a banking partner that can help supply the kind of protections your business needs, Central Bank stands ready to assist businesses and provide services they can depend on.

Interested in learning more?

Contact us today.

Central Bank

Strong roots. Endless possibilities.℠

www.centralbank.net

EQUAL HOUSING LENDER

Member FDIC