AG ADJUSTMENTS

We usually associate credit fraud with the impact it has on individuals in the form of identity theft or phishing scams and the personal financial problems it causes, but what about businesses? What is the incidence of B2B credit fraud and is it a major problem?

Yes, it is a major problem. According to credit reporting agency, Experian, B2B fraud costs US businesses “more than $50 billion annually” and most analysts believe that that number is too conservative. It is also assumed that the incidence of fraud will continue to increase as the use of various electronic payment methods continues to grow.

HOW EXTENSIVE IS THE PROBLEM?

For an overview of the problem let’s take a look at some results from the Association of Financial Professionals (AFP) “*Payments Fraud and Control Survey”*, published in March 2015*:*

Some highlights from this survey are:

- 62% of companies were subject to payments fraud in 2014.
- The most-often targeted payment method by those committing fraud attacks are checks. Check fraud also accounts for the largest dollar amount of financial loss due to fraud.

- The second most frequent targets of payments fraud are credit/debit cards.
- 92% of survey respondents firmly believe EMV- enabled credit/debit cards will be effective in reducing point-of-sale (POS) fraud. EMV- Europay, MasterCard and Visa — is a global standard for cards equipped with computer chips and the technology used to authenticate chip-card transactions.
- 61% of survey respondents believe that Chip-and-PIN validation will be most effective in preventing credit/debit card fraud.

Business fraud can devastate a company and as there are very few external protections it is up to the business to protect itself. A company must be aware of the various types of fraud that it may be subjected to and develop methods for protecting itself.

WHAT ARE SOME OF THE DIFFERENT TYPES OF B2B FRAUD?

There are many different B2B fraud schemes. Here are a few of them:

- **Account Takeover:** This is similar to the phishing and telephone scams that affect personal identities. Here credit card or account information is intercepted and later used to place orders or otherwise defraud a legitimate business. This particular type of fraud accounts for a large percentage of B2B fraud occurrences.
- **Business Identity Theft:** Here a scammer opens business accounts under the name of a legitimate business. The applicant acts as the business owner (or a representative) and utilizes their contact information to apply for credit or open accounts.
- **Commercial Bust-out:** The culprit opens several lines of credit with the intention of eventually abandoning them once the credit limits have been reached. This requires that a good credit history be fabricated so that limits can be increased and maxed out right before the perpetrator disappears. This type of fraud results in millions of dollars of losses every year.

- **Never Payment:** Here a business or individual opens a new account, by materially misrepresenting itself. They will obtain the maximum credit possible, but never make a payment.
- **Shell Companies:** These are companies that are set up solely for the purpose of committing fraud. The entity will not sell a product or provide a service. Many times they are used to launder money. They rarely have a physical location, and if they do, it may be a storefront or offshore.
- **Bleed-outs:** This method of committing fraud is similar to a bust-out. However, it is committed from within by insiders. Employees commit this type of fraud over a long period of time. They bleed out assets, leaving the company unable to pay its bills

SOME CHARACTERISTICS THAT MAY INDICATE A POTENTIAL PROBLEM

Individuals and groups committing these types of frauds will often display many of the same characteristics. The following are some of the things you should look for:

- **Companies without Long Histories:** Typically, companies with longer track records are safer to do business with because they will have more credit history and references to check. The shorter the life of the company, the less you will have to work with.
- **Suspicious Changes in Ownership:** A well-established company, with good credit, is taken over by a new group that tries to hide the change in ownership. This may signal a potential problem. It may be an indicator that members of the new owners are committing fraud.
- **Questionable Financial Statements:** Mistakes or suspicious items on a company's financial statements may be a harmless accounting error or signal a

real problem. A detailed financial analysis is necessary before doing business with this company.

- **Fraudulent Credit References:** False credit references on a credit application are a warning sign to forget about doing business with this applicant. Unless the applicant can prove it's a clerical error and has other good references, doing business with this entity is an invitation to be scammed.
- **No Receivables:** If a company's financial statements do not list any receivables, assuming they are not a cash only business, they are probably a phony shell company that is not providing any goods or services to customers. Do not extend

HOW DO YOU PROTECT YOUR BUSINESS FROM B2B FRAUD?

Validate All Information

The easiest and most important step in B2B fraud prevention is to verify the information provided by companies that want to do business with you. This means you need a credit application (see our blog on credit applications). All the information provided needs to be thoroughly reviewed and verified. Make sure everything on the application is accurate, and ask questions if it is not. Any material errors are a reason not to do business. Additionally, if your business is contacted by a bank, credit card company, or government agency, don't provide any sensitive information before verifying the legitimacy of their request.

Utilize External Credit Sources

A business can pull a credit report on another business to ensure that they are dealing with a credit worthy company. Unlike personal credit, which is protected by the Fair Credit Reporting Act (FCRA), anyone can pull a business's credit report at any time without permission.

Utilize Fraud Detection Tools

Utilizing a fraud detection tool like Experian's National Fraud Database allows you to compare credit applications and other information to current fraud records stored in a national database. If the applicant is in this database, you want to be very careful about doing business with them. COD may be your only option.

Ongoing Transaction Review

Review your banking and credit accounts on a regular basis. Not doing so can leave you and your business a victim of fraud. Initially, transactions tied to fraud or illegitimate charges may not be large enough to indicate a problem, but by monitoring your accounts on a regular basis, you'll be able to spot fraudulent transactions before real damage has been done.

Staff Education

Make sure you educate your employees on the various types of fraud and how to prevent it. You will sleep a lot better knowing your staff has the ability to protect your business against scammers and con artists.

CONCLUSION

B2B credit fraud is becoming more and more of a problem. Important business, financial and personal data are increasingly being compromised. Preventing and defending against B2B credit fraud is a challenge for companies. But you can limit your exposure and minimize losses due to such activity. Being aware of the problem is an outright necessity and implementing the protective measures described above will help reduce most of the risk of B2B credit fraud.