BrightQuery NACM

WHITE PAPER

THE EVOLVING THREAT OF FRAUD IN B2B TRADE

OVERVIEW

Credit fraud is one of the fastest growing challenges for businesses today. 2023 witnessed a rise in various forms of fraud, signaling a pressing challenge for businesses engaged in commerce. These trends have not only put credit managers on high alert but have also underscored the importance of new and robust security measures to safeguard sensitive financial information. Vigilance and adaptability are paramount, as businesses strive to stay one step ahead of the ever-evolving strategies employed by fraudsters.

As fraudsters become more creative with their tactics, the potential for larger losses increases. From sophisticated phishing schemes to identity theft and falsification of financial documents, fraudsters are adapting to technological advancements and exploiting vulnerabilities in digital transactions to target businesses.

As the digital landscape continues to shape the future of B2B trade, the battle against fraud demands a commitment to creative fraud prevention strategies. With each passing day, it becomes abundantly clear that the need for proactive risk management and advanced security protocols is more pressing than ever in the B2B credit domain. Credible, validated information is the best tool available to credit managers to mitigate the risk of fraud.

Overview 2
Key Fraud Findings 3
Sales Business Fraud 4
Current Fraud Trends 5
Business Personas 8
Fraud Red Flags 11
Common Types of Fraud in B2B Trade 13
Future of Fraud 15
Impact of Fraud 17
Fraud Prevention Strategies 18
Fraud Program Key Elements 23

KEY FRAUD FINDINGS

- **Proactive risk management and advanced security protocols** are more pressing than ever in the B2B credit domain.
- **Automated access to third-party information** is the best tool available to credit managers to mitigate the risk of fraud.
- **44% of credit professionals** have seen an increase in fraud attempts from new customers filling out credit applications. Once a fraudster is successful in infiltrating a company, it takes nearly half of all businesses one month to discover the fraud.
- **Nearly 60% of B2B credit managers** have experienced a customer fraudulently dispute a credit card charge.
- **Insufficient Customer or Client Information**: 27% of credit professionals estimate that their company loses more than $1 million dollars each year due to the inability to obtain sufficient customer information.
- **Digital Age of Transactions Opens Fraudulent Opportunities**: From sophisticated phishing schemes to identity theft and falsification of financial documents, fraudsters are adapting to technological advancements and exploiting vulnerabilities in digital transactions to target businesses.
- **Third-Party Private Company Data Sources** are required to verify businesses for financial transactions.

SALES BUSINESS FRAUD

Sales fraud refers to deceptive practices within the sales process that aim to mislead or defraud individuals or organizations.

Here are some common types of sales-related fraud:

- **Fake Information**: Fraudsters create bogus leads with made-up names, companies, or contact details.
- **Recycled Leads**: Old or inactive leads are re-entered into the system, wasting time on unqualified prospects.
- **Bots & Automation**: Fraudulent software generates fake leads automatically, flooding sales teams with useless contacts.
- **Misrepresentation**: Leads might exaggerate their needs or financial capabilities to appear more attractive. Scammers falsely claim to be affiliated with well-known companies or financial institutions. They may impersonate legitimate businesses to deceive consumers. In 2023, people reported losing $752 million to business impostors.
- **High-Pressure Sales Tactics**: Manipulative sales pitches rush buyers into making decisions they may later regret. These tactics can constitute fraud, especially in selling investment opportunities.
- **Financial Statement Fraud**: Fudging important financial numbers (e.g., sales, revenues, assets, liabilities) to deceive credit review and verification of a business size and industry.

The key to detect potential business fraud is to utilize third-party private company data sources that verify a company or legal entity is real and is active operationally.

CURRENT FRAUD TRENDS

Fraud manifests itself in various forms. Fraud trends are notably dynamic and contingent on various factors such as industry, company size and region. Industries differ in their susceptibility to specific types of fraud; for instance, financial services often contend with identity theft and cyber fraud, while manufacturing sectors may face challenges related to supplier fraud or intellectual property theft.

Company size also plays a role, with smaller businesses often targeted for invoice fraud (the manipulation of invoices or billing documents with the intent to deceive for financial gain) or payment diversion due to potentially less robust internal controls.

Regional disparities contribute to the variance in fraud trends, with certain regions experiencing higher instances of fraud types due to cultural nuances or varying regulatory landscapes.

Understanding these nuances is pivotal for businesses, as it allows tailored strategies to combat fraud that align with industry-specific risks, company size, and regional intricacies.

Retail Industry

One prevalent form of fraud involves inventory shrinkage, where goods are pilfered or mismanaged, leading to substantial losses for retailers. Additionally, payment fraud, including chargeback fraud or unauthorized transactions, poses a significant threat, especially in online B2B retail environments.

This is also known as friendly fraud, when a cardholder identifies a purchase on their transaction statement as fraudulent and disputes it sparking the chargeback process. With consumer behavior changing due to the pandemic, digital transactions have increased dramatically resulting in more frequent friendly fraud cases. The risk of credit card fraud typically falls on the credit card company. However, in transactions where the card is not present, most of the risk is on the merchant unless the issuer authenticates it.

Chargebacks on credit cards can indicate various issues, and whether to continue doing business with a customer after a chargeback depends on several factors. Understanding the reason behind the chargeback is crucial. It could be due to a legitimate dispute (product not received, item not as described) or an attempt at fraudulent activity. If the customer has a pattern of initiating chargebacks frequently without valid reasons, it could indicate problematic behavior, and continued business might pose a risk.

Construction Industry

The complicated nature of construction projects, involving multiple entities and intricate supply chains, provides ample opportunities for fraudsters to exploit vulnerabilities.

In the construction industry, a common scheme involves collusion between suppliers and employees, where kickbacks or inflated prices are exchanged, resulting in financial losses for the company. The industry faces the risk of materials theft or substitution, impacting project quality and budgets. Bid rigging and contract manipulation also prevail, compromising fair competition and distorting market dynamics.

Disadvantaged Business Enterprise (DBE) programs are intended to aid small businesses owned by minorities, women, or service-disabled veterans. However, these programs can create holes for fraudsters to take advantage. Whistleblowers under the False Claims Act (FCA) are provided incentives for bringing lawsuits against any enterprise who defrauded government and private entities.

A certain participation percentage is required for disadvantaged contractors to be involved in construction projects. "Anyone involved in a project with a DBE is required to complete due diligence," said Chris Ring of NACM's Secured Transaction Services. "And anyone selling to these contractors now must verify that who they are selling to is a legitimate disadvantaged enterprise. The material supplier can get caught up in a mess and prosecuted under the False Claims Act at the state or federal level if it turns out that they are not selling to a legitimate DBE contractor."

Payment terms can be red flags for fraud when they deviate from industry standards or common practices. "One of the conditions we always look at is the quality of the general contractor (GC) that our subcontractor might be looking to work with," said D'Ann Johnson, CCE, credit manager at A-Core Concrete Cutting, Inc. (Salt Lake City, UT). "We also pay attention to our customer's contract to that GC and see if they're accepting those terms and if they're agreeing to a pay-when-paid or pay-if-paid clause."

Transportation Industry

Bad record keeping can allow fraudsters to take advantage of businesses, Sally Miller-Cheek, senior manager of shared services at BNSF Logistics added. "Sometimes companies are billed for loads they did not move and if they don't have good record keeping and know what they are issuing, they can get billed for items that were not moved."

Depending on the product and time of the year, theft also can be an issue, she added. "Especially if the product is in high demand. Any time of the year with heightened shipping traffic, like Memorial Day weekend and Fourth of July, theft becomes more common."

Breanna Bly, logistics compliance analyst at Trinity Logistics (Seaford, DE), has seen a 200% to 300% increase in crime and fraud in the transportation industry. She said double and triple brokering scams are the most common—and they are not always easy to catch. "When customers come to us to move their freight, we vet them the best we can. But unfortunately, there are still sneaky fraudsters who can still slip through the cracks. There are impersonators who can pretend to have a load that they really don't have and then we go through the process of getting that load moved and at the very end no one is there to pay for the freight that we hauled."

Bly said the transportation and logistics industry has become a target for fraud in recent years. To prevent fraud, it will take support from the entire industry, she added. "Unfortunately, this cannot be entirely fixed from our end. We need the backing from everyone. It helps if the shipper can verify the truck we say is coming in, but when you deal with very large shippers, they can't keep up with every truck. That would be the best defense, but we aren't quite there yet."

Double brokering a load is an illegal practice in the logistics and transportation industry involving multiple freight brokers. In a typical freight brokerage arrangement, a shipper contracts with a broker to arrange for the transportation of goods with the carrier. However, in a double brokering situation, this process has an additional step. Instead of the initial broker contracting directly with a carrier, they engage another broker to find a carrier which the shipper is unaware of. Double brokers typically are legal entities that appear to be a legitimate company but do not have full-time employees or a commercial address. BrightQuery (BQ) has summed the number of "legal entities" in the U.S. There are significant numbers of entities that are legally inactive, have no verified EIN, no verified legal entity registered or no commercial address.

Companies that cannot be verified for legal status, EIN, Commercial address, or economic activity should be further reviewed or maybe avoided.

BQ also summed the number of verifiable indicators such as legal status is active, verified EIN, and has a commercial address. Selecting companies with these verified indicators reduces the likelihood of fraud potential.

Fraud Indicators Compiled by BQ - 4Q2023

COMPANY TYPE	# COMPANIES	INACTIVE	NON EMPLOYER	NO FOUND EIN	NO VERIFIED LEGAL ENTITY	HAS IRS TAX LIEN	RESIDENTIAL ADDRESS
Employer	9,894,880	4,252,013	0	7,338,148	3,731,870	163,433	3,516,983
Holding Company	7,208,266	2,423,803	7,208,266	6,011,590	0	58,895	2,700,426
Non Employer	3,593,752	1,223,928	3,593,752	2,937,873	71,730	38,628	1,649,851
Sole Proprietor	53,339,592	28,429,751	53,339,592	48,106,442	616,776	158,071	26,924,929
Total	74,036,490	36,329,495	64,141,610	64,394,053	4,420,376	419,027	34,792,189
Employer	13%	6%	0%	10%	5%	0%	5%
Holding Company	10%	3%	10%	8%	0%	0%	4%
Non Employer	5%	2%	5%	4%	0%	0%	2%
Sole Proprietor	72%	38%	72%	65%	1%	0%	36%
Total	100.0%	49.1%	86.6%	87.0%	6.0%	0.6%	47.0%

Potential fraud indicators are separately summed.

BUSINESS PERSONAS

Developing and understanding basic types of businesses or "personas" reveals which businesses have greater barriers to entry or formation vs those that have few barriers. Businesses that have significant barriers to form require significant capital, a commercial location, have full-time employment, and offer benefits from the start.

Businesses that require none of these qualities are more likely to be used to commit fraud or have little resources to afford to purchase goods and services. It only requires a nominal fee to create a legal entity registered to a PO Box, private mailbox service, or a residential address.

Bright Query provides fraud indicators to verify any company or legal entity for full-time employees, a commercial address, its industry, and many other qualities for an automated review.

BQ - Select Business Persona Types and Likelihood of Fraud

BUSINESS PERSONA	DESCRIPTION	TYPICAL BUSINESS QUALITIES					
		CAPITAL INTENSIVE?	COMMERCIAL ADDRESS?	HAS FULL-TIME EMPLOYEES?	OFFERS BENEFITS?	TYPICAL NAICS SECTOR	FRAUD LIKELIHOOD
Standard	Normal business that has only commercial address, employment.	Yes	Yes	Yes	Yes	Various	Low
General Contractors	A general contractor oversees commercial or residential construction projects. They act as project managers and coordinate a group of subcontractors.	Yes	Yes	Yes	Yes	Construction	Low
Subcontractors	Subcontractors specialize within the construction trade. They take contracts from the main contractor for work that exceeds the main contractor's skill level.	No	Residential & Commercial	Yes	No	Construction	Below average
Service Oriented	Service companies are businesses that generate income by providing services, not physical products, to their customers such as house cleaning, maintenance, accounting, transportation, telephony, and more.	No	Residential & Commercial	No	No	Various	Below average
Independent Contractors	Similar to business owners, independent contractors work for themselves.	No	Primarily Residential	No	No	Agriculture, Mining, Administration, Accommodation & Food Services, Other Services	Average
Brokers	A broker is an intermediary who helps perform financial transactions on behalf of a client. Brokers can be individuals or firms.	No	Residential & Commercial	No	No	Finance & Insurance, Real Estate	Average
Associations & Organizations	Legal entities that promote the interests of their members.	No	No: Primarily Residential	No	No	Other Services	High
Non Profits	A nonprofit organization (NPO), is a legal entity organized and operated for a collective, public, or social benefit. Tax-Exempt Status: 501 (c)(3) status	No	Residential & Commercial	No	No	Other Services	High
Holding Company	Legal entities that do not have economic activities but are legally in good standing.	No	No: Typically no operational address	No	No	Management of Companies	High

BQ - Company Characteristics for Business Verification

COMPANY TYPE	# COMPANIES	ACTIVE	EIN	COMMERCIAL ADDRESS
Employer	9,894,880	5,642,867	2,556,732	4,860,772
Holding Company	7,208,266	4,784,463	1,196,676	2,444,569
Non Employer	3,593,752	2,369,824	655,879	1,428,724
Sole Proprietor	53,339,592	24,909,841	5,233,150	15,974,887
Total	74,036,490	37,706,995	9,642,437	24,708,952
Employer	13.4%	7.6%	3.5%	6.6%
Holding Company	9.7%	6.5%	1.6%	3.3%
Non Employer	4.9%	3.2%	0.9%	1.9%
Sole Proprietor	72%	33.6%	7.1%	21.6%
Total	100.0%	50.9%	13.0%	33.4%

Indicators are separately summed.

There are over two million companies that have in combination a verified commercial address, an EIN, and are active. These businesses also file employment records and are highly verifiable.

COMPANY TYPE	# COMPANIES	% OF TOTAL COMPANIES	COMMENTS
Employer	1,072,967	1.4%	Highly Verified
Holding Company	268,445	0.4%	No economic activities
Non Employer	207,829	0.3%	No associated employment filings
Sole Proprietor	804,563	1.1%	Not full-time employers
Total	2,353,804	3.2%	

Companies that have a commercial address, a verified EIN and are active

State regulation and varying restrictions to register and operate a business cause differences in the average fraud indicators per company. Florida, for example, not only has the highest average but also the largest share of potentially fraudulent businesses. It is also a state with one of the highest prevalences of consumer fraud according to the Federal Trade Commission.

BQ – TOP FIVE STATES WITH THE HIGHEST FRAUD INDICATORS

FRAUD INDICATORS PER COMPANY

STATE	AVG FRAUD IND PER COMPANY	% OF TOTAL FRAUD INDICATORS
Florida	1.61	14.5%
Puerto Rico	1.34	0.1%
North Dakota	1.25	0.1%
California	1.25	8.2%
Massachusetts	1.24	1.6%

TOTAL FRAUD INDICATORS PER STATE

STATE	TOTAL FRAUD INDICATORS	% OF TOTAL FRAUD INDICATORS
Florida	12,978,430	14.5%
California	7,342,336	8.2%
Texas	5,722,233	6.4%
New York	5,316,701	5.9%
Delaware	3,196,302	3.6%

BQ – BOTTOM FIVE STATES WITH LOWEST FRAUD INDICATORS

FRAUD INDICATORS PER COMPANY

STATE	AVG FRAUD IND PER COMPANY	% OF TOTAL FRAUD INDICATORS
Wyoming	1.08	0.5%
Delaware	1.12	3.6%
Nevada	1.12	1.2%
Oklahoma	1.13	0.9%
Louisiana	1.13	1.4%

TOTAL FRAUD INDICATORS PER STATE

STATE	TOTAL FRAUD INDICATORS	% OF TOTAL FRAUD INDICATORS
Puerto Rico	46,256	0.1%
Alaska	126,242	0.1%
North Dakota	131,940	0.1%
Vermont	162,270	0.2%
South Dakota	167,321	0.2%

FRAUD RED FLAGS

Fraud presents itself in many ways, but there are also many different warning signs that signal fraudulent activity is in progress. Unusual patterns in transaction behavior, such as sudden changes in purchase volumes or frequencies, deviations from typical buying patterns or repeated last-minute changes in payment methods, can indicate fraudulent intent. If something sounds too good to be true, it's because it probably is. "Fraud is becoming increasingly more difficult to catch," said Alaina Worden, CCE, credit and collections manager at CECO, Inc. (Portland, OR). "Fraudsters are becoming more sophisticated and prey on any company that may have weak spots into their processes."

The fraud triangle is a conceptual framework developed by criminologist Donald Cressey to explain the factors that contribute to fraudulent behavior within organizations. It consists of three key elements that are believed to be present when an individual commits fraud:

1. **Pressure or Incentive**: The first side of the triangle refers to the pressure or motivation that drives an individual to commit fraud. Financial difficulties, personal debts, job dissatisfaction or a desire for a lavish lifestyle can create pressure, leading someone to consider fraudulent actions as a solution to their problems.
2. **Opportunity**: The second side of the triangle represents the opportunity or circumstances that enable someone to commit fraud without detection. Weak internal controls, lack of oversight, inadequate segregation of duties or loopholes in processes provide the opportunity for individuals to exploit vulnerabilities and engage in fraudulent activities.
3. **Rationalization**: The third side of the triangle involves the rationalization or justification that individuals use to morally or psychologically justify their fraudulent actions. They might convince themselves that the act is a temporary loan, justified by a perceived injustice or even believe they will repay the stolen funds eventually.

We cannot change the ill behavior of fraudsters, but companies can develop a fraud review process to verify if a company is real, operationally active, and has sufficient resources to pay its bills.

By recognizing and addressing the factors outlined in the fraud triangle, organizations can establish a robust anti-fraud environment that reduces the likelihood of fraudulent activities and encourages a culture of integrity and compliance.

Below we explore some of the most common red flags for fraud:

Age of Business

A new business seeking credit can raise red flags for potential fraud due to the lack of established financial history and track record. For creditors or suppliers, extending credit to a new business involves an inherent risk, as there's limited or no historical data to assess the new entity's creditworthiness or payment reliability. Fraudsters may exploit this situation by establishing fictitious businesses or shell companies, seeking credit with no intention of fulfilling payment obligations.

Gweneth Weeks, operations manager at Big D Concrete, Inc. (Dallas, TX), said she has received several credit applications for brand new companies or companies that are exactly one year established. In some cases, new customers can also be old friends. "I've noticed the principal of a certain company was a person associated with a different company I've dealt with in the past," Weeks said. "They didn't handle business properly and left behind a lot of unpaid suppliers. So, that was a flag that stuck out to me."

Customer Is Rushing the Order

When a business rushes to secure quick credit approval, it often raises red flags for potential fraudulent intent due to the unusual urgency or pressure applied in the transaction. Fraudsters may manipulate situations by creating a sense of urgency, pressuring lenders or creditors to expedite credit approvals without adequate due diligence. "If the customer is pushing to get a quick approval is also an indicator of fraud," said Kim Hanlin, credit manager at Kloeckner Metals Corporation (Dallas, TX). "Most customers who have terrible credit don't even apply for open terms."

Inconsistent Customer Information

If you are not careful, details such as address changes and email domain inconsistencies can put your company at risk of falling victim to fraud. For example, if an email says gmail.UK instead of gmail.com, you know something is not right. "If it's not a company name in the domain, that also throws up a red flag for us and we'll have to do more due diligence just to double check that one, it is a legitimate company overall and two, that company is applying themselves and not through a fraudster," said Roxanne Price, CCE, CCRA, NACM chair elect and corporate credit manager at H&E Equipment Services (Baton Rouge, LA).

Make sure to research that there are no shell companies tied to the company establishing credit, validating business endorsements with state records that are active and filed. Also, assure UBI and EIN/TIN number for the company name matches IRS and state records, officers of the company are listed on the credit application and, if company website is provided, make sure the domain is active and registered.

If a business has multiple listings at the same location, it should set off alarm bells. "Additionally, if you find multiple credit reports for the same business name and the only difference is LP, LLC, Inc. or LTD, then I always search and identify which entity (or entities) have an active business/corporate status with the Secretary of State," said Brett Hanft, CBA, credit manager at American International Forest Products LLC (Beaverton, OR).

Change in Payment Behavior

Out of character demands for credit can often be a sign of fraudulent activity. Typically, this change manifests as deviations from established patterns or norms in payment schedules, methods, or frequencies. For instance, if a long-standing client abruptly alters their regular payment method from traditional bank transfers to unusual or less traceable methods like cryptocurrency, it could indicate an attempt to obscure transaction trails, raising suspicions of fraudulent intent. Similarly, unexpected delays in payments after a history of punctual settlements or sudden requests for irregular payment terms without valid explanations may also signify underlying issues or attempts to exploit vulnerabilities for fraudulent activities. Monitoring and scrutinizing alterations in payment behaviors can be pivotal in identifying and preventing potential fraud, prompting businesses to delve deeper into these changes and ensure the legitimacy of transactions.

If any customers are using credit cards too much as a supplement for cash, maxing out credit lines and opening several accounts within a short period of time—it could be a cover for fraudulent activity. For instance, sudden alterations in buying patterns, such as a notable increase in order volume, purchases of unusual items or frequent changes in delivery locations, could be indicators of potential fraudulent intent. Another warning sign is receiving applications from out of the area of business, which applies mainly to material suppliers. If a customer is ordering shipments out of the area or is willing to pick up large orders using their transportation, that's typically a red flag.

These alterations from typical customer behavior patterns can alert businesses to potential risks, prompting them to conduct further investigations or implement heightened security measures to prevent or detect fraudulent activities.

COMMON TYPES OF FRAUD IN B2B TRADE

The real-life cases discussed in this chapter have been distilled into a variety of situations, circumstances and occurrences that, when identified, most often result in financial losses involving credit. This chapter's objective is to describe those known circumstances that most frequently reveal the trail of fraud and help credit professionals identify the steps necessary to protect their firms from financial loss through credit risk.

Bust-Out Fraud

Some customers will build trust by completing several small transactions over a period and then request a large transaction that was their goal all along—known as bust-out fraud, or sleeper fraud. The fraudster makes on-time payments to maintain a good account standing with the intent of bouncing a final payment and abandoning the account. During the process, the fraudster builds up a history of good behavior with timely payments and low utilization. Over time, the fraudster obtains additional lines of credit and requests higher credit limits. Eventually, the fraudster uses all available credit and stops making payments. Overpayments with bad checks are often made in the final stage of the bust-out, temporarily inflating the credit limit and causing losses greater than the account credit limit.

In a classic bust-out, a company is contacted by someone with an offer to buy large quantities of merchandise with cash on delivery terms. The supplier delivers the goods in exchange for a check drawn on a business account. When the check is returned for insufficient funds, the customer makes apologies for the mistake and sends another check. Often, by this time, another truckload of goods is on its way, but subsequent checks have no more cash behind them than the first. The accounts are real but unfunded. By the time the supplier realizes they've probably been taken, the stolen goods have been sold and the company has skipped out or disappeared.

"Synthetic companies would get credit for small dollar amounts on those accounts and with that credit, they'd pay it for a couple of months," explained a payment risk and fraud director. "We figured out the customer sold the account to someone else, and that person would apply for credit and do a bust-out."

Credit Card Chargebacks

Credit card payments are becoming more common in B2B trade, which means credit professionals must understand the risk that accompanies different payment methods. Customers can ask for chargebacks, a charge returned to the payer in a transaction after they flag an item on their account. They can claim that the goods never arrived, or the

item received was different from what was described, damaged, or the purchase was never authorized by them. This makes it harder for creditors to collect on disputes. An NACM *eNews* poll revealed that 59% of credit professionals have experienced a customer fraudulently dispute a credit card charge.

For in-person transactions, ensure that the information matches to avoid fraud like identity theft or faulty credit cards. "We require that the customer's driver's license match the name on the credit card present," said Anne Scarcella, CCE, CCRA, credit manager at Crawford Electric Supply Company, Inc. (Spring, TX), who does not accept credit cards over the phone for any orders at her branches. "If the customer gives us any pushback or the ID number, name or credit card does not align, we will only process the sale on cash terms."

Fake Credit Applications

An NACM *eNews* poll revealed that 44% of credit professionals have seen an increase in fraud attempts from new customers filling out credit applications. "Traditionally fraud came from existing accounts, but as we've gotten better at catching those, the newest wave seems to be fraudulent applications," said an NACM member. "On the application, these fraudsters are providing just enough accurate information to make it look realistic, while slightly changing letters or acronyms."

Counterfeit Checks

Check fraud is a challenge given the advent of inexpensive desktop publishing systems, laser printers and color copiers. An individual con man can manufacture checks quite easily.

The following tips may help spot forgeries and save costly errors in trusting too much in appearances. Part of the trick in catching check forgeries is to focus special attention on those accounts with these warning signs for potential bad checks:

- Check numbers do not change.
- Checks drawn on new accounts.
- Checks with no account or routing number.
- Inverted watermark on paper.
- Misspelled words.
- Poor printing quality.
- Checks presented near the end of the business day by customers who seem unwilling to wait until the next business day for their order.
- Checks received from customers whose accounts are themselves suspect.
- Normal checks presented to honor a previously submitted bad check.
- Irregular signatures, such as those with an interruption or gap where the pen has lifted off the paper completely.
- First four digits of routing code are not valid.
- District in routing code does not match District in transit number.
- Bank identification number in routing code does not match bank identification number in transit code.
- Check identification in optical scan numbers at bottom of check does not match check number on face of the check.

Identity Theft

Fraudsters can convince customers to change bank account information, so the money is wired to the incorrect account number. Mark Teeter, CCE, CICP, global credit director at ESCO Group LLC (Portland, OR) said fraudsters have even gone as far as posing as ESCO employees. Then they email customers to "have them change the banking address or ACH details of where they pay us," he explained. "This steals from unsuspecting customers and makes it very difficult for us to collect on our owed balances. Most customers will catch this and confirm directly with us, but we've had a couple fall prey to five and six figure payments."

"We are seeing companies that use ACH or wire are receiving spoof emails asking them to change the bank and account number," said Jay Goree, director of credit at Hood Industries (Hattiesburg, MS). "The company has stopped two attempts in the past two months—and has informed customers to not change their remit address without consulting the company first."

Phishing Scams

As one of the most popular forms of communication in the work world, email provides an instant way to get your message across and conduct business. Several advantages come with email communication and almost all workplaces use the tool to communicate internally and externally. In fact, 75% of credit professionals said they use email as their primary form of contact with customers.

However, the surge in phishing scams via email has emerged as a pervasive threat, targeting individuals and businesses alike. These deceitful tactics involve cybercriminals posing as legitimate entities, crafting sophisticated emails that lure recipients into divulging sensitive information or clicking on malicious links.

With increasingly convincing disguises mimicking trusted organizations or urgent messages requiring immediate action, these scams have witnessed a sharp rise. From fake invoices to false security alerts, phishing emails aim to exploit human vulnerabilities, seeking access to confidential data or to install malware.

FUTURE OF FRAUD

With each passing day, it becomes abundantly clear that the need for proactive risk management and advanced security protocols is more pressing than ever in the B2B credit domain. "I think all types of fraud are on the rise partially because the opportunity is there and the risk of getting caught or punishment is low," said Scott Dunlap, director of credit and collections at Coleman Oil Co. (Lewiston, ID). "There are a lot of gaps that were caused by the sudden change in businesses from COVID-19 that have never been properly recognized and resolved."

Here we explore the current factors that are shaping the future of fraud:

Less Staff, More Pressure

Many companies continue to struggle with a lack of resources and staff now more than ever—which can create the perfect breeding ground for fraud. With limited personnel available to oversee operations, the strain on existing employees can lead to increased workloads and a lack of adequate oversight across various departments. This situation creates fertile ground for obvious red flags to go undetected.

In a fast-paced business world, customers are looking to get credit approval as quickly as possible—and the credit department is under pressure to make a fast decision to secure the sale and unlock revenue, while maintaining the same level of due-diligence. With an increase in the number of credit applications coming through credit departments, there is a need to move quickly to get an account set up. But this mindset can create opportunities for fraudsters.

Outsourcing, while a common business practice to streamline operations and reduce costs, can inadvertently open avenues for B2B fraud if not managed diligently. Entrusting critical business functions or sensitive processes to third-party vendors without adequate oversight or monitoring can create vulnerabilities. Lack of direct control or supervision may lead to lapses in security, allowing fraudulent activities to go unnoticed.

Digital Age

Our increasingly interconnected digital world has presented both opportunities and challenges. Technology has opened avenues for fraudsters to exploit, especially with the rise in popularity of digital credit applications.

"We have seen a massive jump in fraud attempts during the new customer setup process as we started offering an online credit application," one NACM member said. "Traditionally, someone would come into a branch, call or email and ask for an application. But now [new customers] can just go online and that is where they have been able to easily put in fraudulent information."

"There shouldn't be a difference between the digital and paper credit application processes when the information is analyzed the same," said Anton Goddard, president at NACM South Atlantic (Orlando, FL). "However, it's up to the credit manager to reach out to their sales staff and ask questions as part of the digital credit application review process. Asking questions about the business location, the staff and their impressions should always be considered."

"In the past three years, we've seen more attempts from fraudsters to try and submit fake data to the National Trade Credit Report (NTCR) than ever before," Goddard said. "The trend we've seen recently is companies that open internet stores try to entice people to open an account with 30-day terms and then try to report that information to NACM, but we are not accepting trade data from these people for credit building purposes."

Digital credit applications are more susceptible to fraud because the personal relationship between the company and the applicant is substantially diminished. "I recently looked at late paying accounts and 85% were from inside sales that had no personal visit by the sales reps and were unsolicited applications received electronically," Dunlap said. "Digital applications are efficient and convenient, but nothing replaces the personal relationship."

In-person customer visits—once a standard practice in B2B credit management—are no longer as common given the digital age. Most credit professionals agree that in-person customer visits will continue to decline with the rise of technology, said Alicia Johnson, CBA, CCRA, credit supervisor at Cleveland-Cliffs Steel (Burns Harbor, IN). "Although they are valuable, we might see less and less of them as people are adapting to technology and getting more comfortable with putting their trust in us."

Lack of Training

Some credit departments are still lagging in training after the COVID shutdowns. Working from home is convenient, but people still learn from each other in groups and collaborative environments. Credit departments were already receiving minimal training about fraud and that standard has dropped even lower in recent years. When stakeholders, whether individuals or organizations, lack sufficient understanding of industry norms, transaction processes, or the evolving methods employed by fraudsters, they become susceptible to manipulation and exploitation. Investing in education, continuous training, and staying abreast of emerging fraud trends becomes pivotal in fortifying B2B trade against fraudulent activities.

Volatile Economy

From boom times to economic downturns, fraudsters adapt their tactics to exploit vulnerabilities and capitalize on changing circumstances. Understanding these fluctuations is paramount for businesses and individuals alike, as it allows for proactive measures to mitigate risk and safeguard assets.

With economic stress and factors such as labor shortages, it can cause both credit managers and customers to cut corners, allowing fraud to slip through the cracks. Whether it is too many people assigned to the task of new customer setup or just the urgency in business and competition, credit professionals must take an extra step to ensure security. In slower seasons of business, more fraud can leak through because some companies may overlook red flags in exchange for added sales.

The COVID-19 pandemic has accelerated the pace of technological adoption across industries, revolutionizing the way businesses operate and individuals interact. While this rapid digital transformation has brought forth numerous benefits and opportunities, it has also provided fertile ground for fraudulent activities to thrive.

One of the main drivers of fraud after COVID-19 is increased reliance on digital platforms and remote communication channels. With the widespread adoption of remote work and online transactions, cybercriminals have leveraged phishing attacks, malware and social engineering tactics to target individuals and organizations.

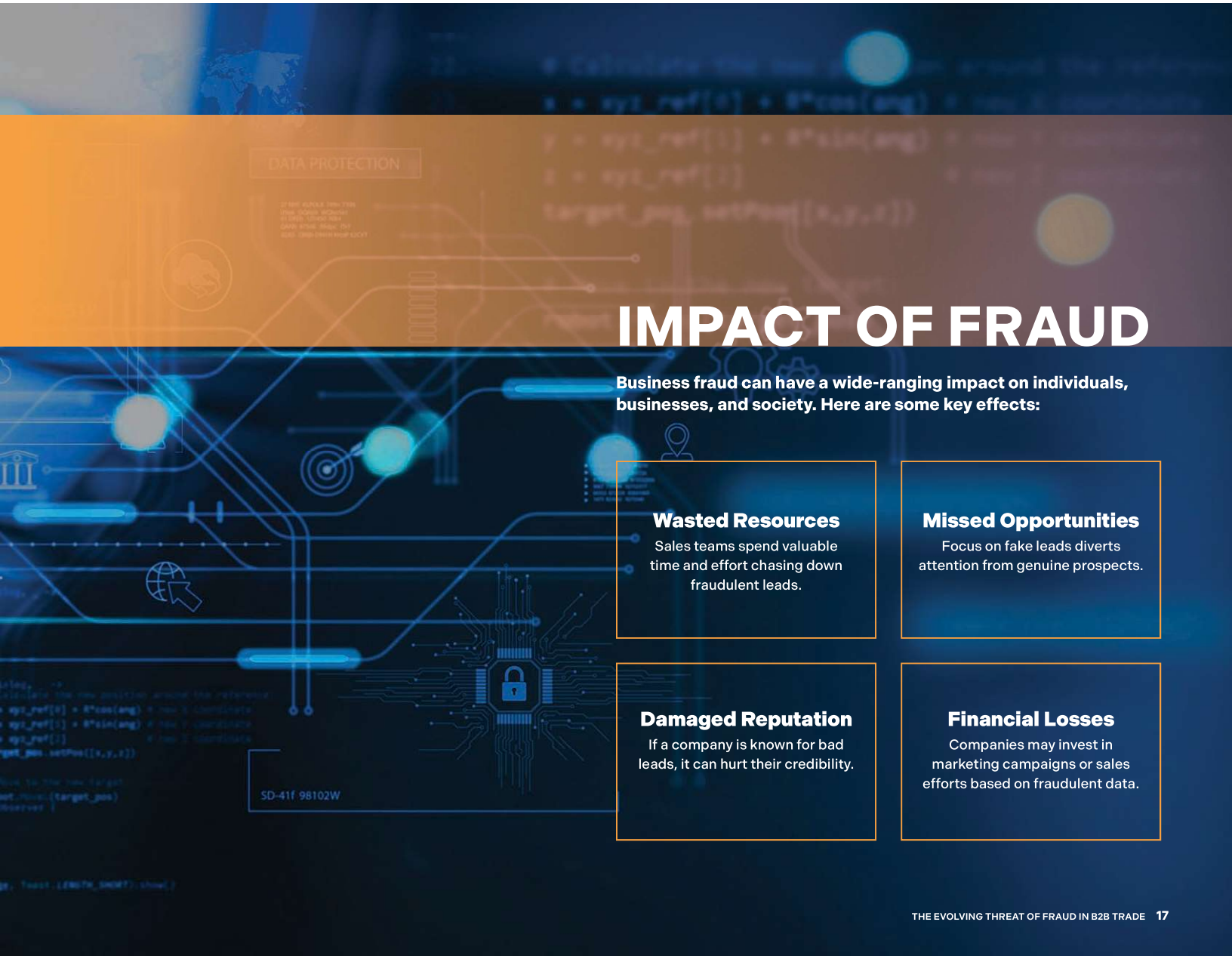
Cyber Liability Provisions

Cyber liability provisions can change frequently as it is a newer concept. There is not enough case law yet to determine what exact provisions should be included in those contracts. Some contracts under cyber liability provisions can include language that holds your company responsible if your customer falls victim to fraud by someone else pretending to use your company's name. "This provision is assigning risk and liability, but it can be misleading," Steve Winn, corporate credit manager at Marek Brothers Systems, LLC (Houston, TX). "Even if we're a solid company and doing everything right, fraud could still happen and could hurt for us."

If a contract does include cyber liability indemnity provisions, your company could be responsible for financial damages from data breaches that originated from your system (through a phishing email link, for example). A data breach could cost millions of dollars, said Winn. "What we're seeing is provisions that are in a broader form, with some that only apply if you're integrating your system with another company's system," Winn added. "Secondarily, we have interest requirements that are requiring cyber liability coverage for between $1-$5 million and it's becoming increasingly hard to obtain at a reasonable price."

Artificial Intelligence

As AI capabilities evolve, fraudsters may exploit these same technologies to develop more sophisticated and adaptive fraudulent tactics. They could use AI to generate more convincing phishing scams, create fake identities, or manipulate algorithms to evade detection. Over-reliance on AI-driven systems without human oversight might lead to complacency. Trusting AI to handle all aspects of fraud detection without human verification could result in overlooking nuanced or complex cases that require human judgment. AI-driven fraud detection systems often require access to vast amounts of personal data. Balancing the need for effective fraud prevention with privacy concerns poses ethical challenges and requires robust data protection measures.



IMPACT OF FRAUD

Business fraud can have a wide-ranging impact on individuals, businesses, and society. Here are some key effects:

Wasted Resources

Sales teams spend valuable time and effort chasing down fraudulent leads.

Missed Opportunities

Focus on fake leads diverts attention from genuine prospects.

Damaged Reputation

If a company is known for bad leads, it can hurt their credibility.

Financial Losses

Companies may invest in marketing campaigns or sales efforts based on fraudulent data.

FRAUD PREVENTION STRATEGIES

Access to information is the best tool available to credit managers to mitigate the risk of fraud. As new types of fraud emerge, you will need to change your processes accordingly as you learn new ways these people are going to commit fraud and remain flexible to catch every new attempt. It is key to develop a thorough, written fraud prevention plan that everyone at your company understands and can follow before, during and after fraud.

Delegation of Authority

Delegation of authority is the action of transferring the responsibility of a task to another individual. In the workplace, delegation is an essential management skill, playing a role in business productivity, team performance and empowerment to employees within the organization. But arriving at final business decisions is still a team effort. Because of the risk involved in making credit decisions, leaders should still ensure a few helping hands in making decisions. Some managers may work directly with other departments, but others make the final say themselves.

This includes involving senior management in a credit decision once a customer requests a certain dollar threshold. For example, you might need certain data points to approve a $30k credit limit but need additional information to approve a higher limit.

Involve Your IT Department

Passwords act as the frontline defense against unauthorized access and fraudulent activities in the digital realm. By frequently changing passwords, individuals and organizations minimize the risk of compromised accounts due to breaches, phishing attacks or unauthorized access. It disrupts potential hacking attempts and limits the window of opportunity for fraudsters to exploit stagnant credentials. Changing passwords regularly,

employing strong and unique combinations, and utilizing multifactor authentication significantly fortify security measures, mitigating the risk of identity theft, financial fraud and unauthorized access to sensitive information.

Always check your spam and junk folders. Some companies have policies in place to report or delete suspicious messages altogether. "Security wise, we have automatic notifications from our IT department where any email headings sent from an outside network will come with an immediate warning," said Wesley Belleville, CCE, CICP, director of credit at Helena Agri Enterprises, LLC (Collierville, TN). "It gives us a heads up on exactly who you are sending to or receiving from. All unknown emails go to an automatic spam folder created by our company that captures emails and places those into the folder."

Get Creative

Some credit managers put warnings in their email signatures so that all customers are made aware of the fraud attempts. For example, including the following message would alert customers: We have recently learned that fraudsters pretending to be [insert company name] credit team members are emailing customers to set up ACH payments and change bank account information to steal future payments. These communications come from email addresses that are similar to our domain to make them harder to detect. These communications are not from us. All payments should continue to be sent to the remittance address you have on file.

The same verification process applies to online orders. Scarcella has a digital team with a standard operating procedure (SOP) that processes online orders. "We have turned down many orders of suspected fraud," she added. "But even then, we have our fair share of chargebacks under the 'fraud' category."

Collaborate with Other Departments

The sales team can be valuable in preventing fraud, Teeter said. "Our sales teams do physically vet any customers before sending applications through, so that may be the best defense, and I always dig a little deeper online to vet out addresses and potential trade references that aren't listed on the application."

Other than independently verifying information, members recommend involving the local sales or credit department that work in the area where the application is from. "You cannot rely on just people's titles and names anymore because that information can easily be taken."

Research Information

A few of these fake accounts made it through one NACM member's credit department, and their team has since been on high alert. "We are operating on heightened security," she said. "Our team has been checking independent sources to verify information of the company applying for credit and contacting the company directly. We check to see if the person applying is truly their employee."

Sometimes it takes a simple internet search or social media to catch a fraudster trying to set up a fake account, said Tim Cain, CBA, director of global credit and collections at KEEN Inc. (Portland, OR). "We review the credit app and check references, Google search 'bill to' and 'ship to' locations, LinkedIn search owner, etc."

Some credit professionals use built-in fraud check verification processes during the new account setup. Vimal Patel, CBF, regional credit manager at OneSource Distributors, LLC (Oceanside, CA), said he no longer gives out their company's full wire instructions in writing. "We give the instructions partially and customers and vendors have to call for the remaining portion," he added. "We run a daily credit card report that is sent out to all our sales managers and their respective operations managers so they can review and flag any potential fraud transactions before we ship out the material."

Credit Industry Groups

Networking is another tried and true strategy for catching fraud. By participating in NACM industry groups and meeting with other credit professionals, one member was able to "compare notes and realize a pattern of one person attempting to set up an account and purchase copper wire from multiple businesses," they explained.

"We didn't really use the internet until fraudsters started filling out our credit applications to obtain parts or equipment," said Heidi Lindgren-Boyce, CCE, senior credit manager at Star Rentals, Inc. (Kent, WA). "We previously relied on credit reports but started moving towards searching the addresses and complaints part of the internet and once COVID hit, it's become an active resource when vetting new customers."

Credit Reports

If you are unsure about a credit application, it is always best to order a credit report from a trusted organization. NACM's National Trade Credit Report (NTCR) is your one stop shop for reliable credit information. "As a credit detective, my ability to put the clues together for a good credit decision just got a whole lot easier," wrote Norman Zusevics, CICP, manager of credit risk assessment at Shure (Niles, IL).

5 Cs of Credit

The 5 Cs of credit—character, capacity, capital, conditions, and collateral—form a fundamental framework for evaluating creditworthiness. While primarily used for assessing the likelihood of repayment, these principles can also contribute to fraud prevention.

Character: A thorough assessment of character can help detect red flags or inconsistencies in behavior that might indicate potential fraudulent intent. Consistent and reliable behavior over time could signal a lower likelihood of engaging in fraudulent activities.

Capacity: Analyzing capacity involves understanding financial statements and transaction histories. Inconsistencies or irregularities in financial records might hint at potentially fraudulent activities, prompting further investigation.

Capital: Adequate capital reserves can act as a safeguard against defaults caused by fraud or financial instability. For instance, a lack of capital or sudden depletion could raise concerns about potentially fraudulent activities that lead to financial strain.

Conditions: Understanding prevailing market conditions aids in identifying potential fraud risks. Unusual or unexpected shifts in market conditions could necessitate closer scrutiny, as they might indicate fraudulent activities manipulating the market.

Collateral: While not directly related to fraud prevention, adequate collateral can mitigate financial losses resulting from fraudulent activities. However, fraudulent collateral or misrepresentation of its value could signal attempts at deception or fraud.

In-Person Customer Visits

In-person customer visits have existed since the birth of credit management as a method of gathering information, collecting payment, and building customer relationships. But with the advances in technology and a global pandemic, in-person customer visits may become a thing of the past.

According to an *eNews* poll, more than half (63%) of credit professionals no longer conduct customer visits as part of their credit investigation. But for the 37% of credit professionals who still visit customers face-to-face, they say the value gained is unmatched. Meeting customers face-to-face allows for visual identity verification. This helps confirm that the person you are interacting with matches the identity provided in documents, reducing the risk of identity theft or impersonation. Observing a customer's physical location, business operations, or assets during an in-person visit provides insights into their legitimacy. It helps verify the existence of the business, assets, or operations claimed in documents, reducing the risk of fraudulent representations.

Automate Your Credit Process

BrightQuery (BQ) is a data solutions company that operates in the financial and business services sectors. It manufactures a business database on all U.S. companies and legal entities sourced only from government filings.

This accurate and up-to-date dataset includes quarterly financials, monthly headcount and payroll, benefit plans, private stock filings, and firmographics based on government filings.

The company primarily serves the banking, insurance, hedge fund, asset management, sales and marketing, and commercial real estate industries.

BrightQuery has designed a robust Fraud & Compliance system tailored for KYB/KYC protocols.

This system offers comprehensive checks ranging from the legal status of entities with the Secretary of State to verified employment status with the Department of Labor; from verification of the business address type to financial filings to the IRS, providing a fortified layer of verification and compliance assurance.

The BQ Fraud Indicator System can automatically perform the following checks:

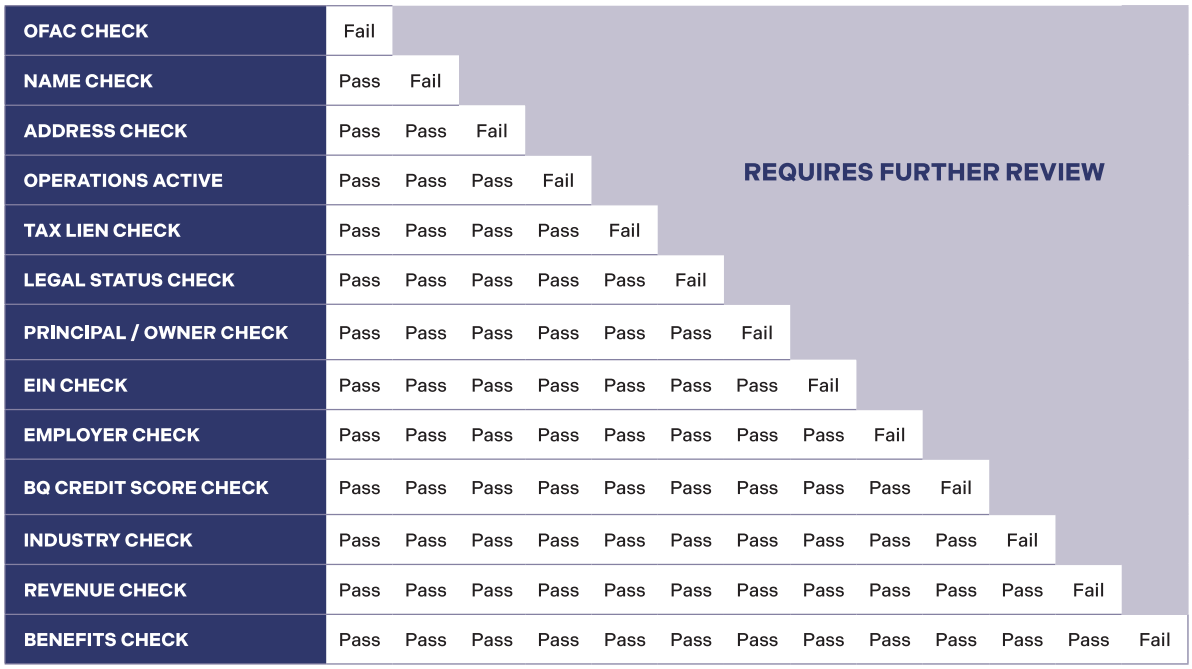
According to an *eNews* poll, more than half (63%) of credit professionals no longer conduct customer visits as part of their credit investigation. But for the 37% of credit professionals who still visit customers face-to-face, they say the value gained is unmatched.

BQ – FRAUD INDICATOR SYSTEM

FRAUD CHECKS	ACTION	LEGAL ENTITY VERIFICATION	ADDRESS VERIFICATION	OPERATIONS VERIFICATION
Name & Address	Verification of company name and address	x	x	
Organization Status	Are all legal entities with an organization in good legal standing with the State?	x		
Legal Entity Status	Is the company legally in good standing with the state?	x		
Economic Status	Is the company actively filing with the USDOL or IRS?			x
EIN - Employer Identification Number	Verification of the company's EIN	x		x
Principal/Owner	Principals & officers registered with state	x		
No Officers Registered with Legal Entity	The company reported no officers with the state	x		
Company Type	Is the company an employer, a holding company or a sole proprietor?			x
Benefit Plans	Does the company file benefit plans?			x
Commercial Address	Does the company have a commercial address?		x	
PO Box, USPS, or Private Mailbox	Does the company list a PO Box or Private mail box as its address?		x	
Vacant Address	Is the company's address reported as vacant by the USPS?		x	
Multiple Legal Entities Registered at a Residential Address	Count the number of legal entities registered at a residential address		x	
Tax Lien	Does the company have an IRS Income Tax lien?			x
OFAC	Is the company on the terrorist watch list?			x
Revenue	Compare BQ revenue vs company reported revenue on application			x
Industry	Industry filed by company vs reported by company			x
BQ Credit Score	Credit risk rating of the company			x

BQ fraud indicators are sourced from reported data filings to state and federal government agencies that are used to verify a company's legal standing, its operating address, and economic activity.

The BQ advantage for identifying potential fraud is available without requesting information from the company in question. The example automated fraud detection process helps categorize companies that are likely to be "real" vs ones that are more likely to be "fake."



A standardized fraud check program may systemically improve engagement with verified companies vs engaging with potentially fraudulent players.

FRAUD PROGRAM KEY ELEMENTS

Before engaging or transacting with a company, verify its name, address, and its operations.

The businesses legal entity verification

The goal is to understand if the company currently is real and is registered by a government agency:

- Verify the company name.
- Verify if the company's legal entity is in good standing and active.
- Verify for a larger company if any of its subsidiaries' legal entities are inactive.
- Verify its EIN or its Employer Identification Number
- Who are the Principals or Officers registered?

Summary: Legal entities sign contracts and knowing if they are of good legal standing and the registered owners and officers is key. Companies that have EIN's are further demonstration of verification as EIN's assigned by the IRS are used to hire employees, open bank accounts, and apply for business licenses.

Verify the company's address

- Is it a commercial, residential, or unknown address?
- Is the address a private mailbox such a UPS store or a USPS PO Box?
- Are multiple companies registered at the same residential address?
- Is the address listed as vacant?

Summary: Ideally, a verified business has a commercial address that is active for delivery. Fraudulent companies often use PO boxes or private mailboxes located in stores as addresses. Companies should also be verified if they are operationally active.

Verify its economic activities such as employment, company type, benefits, etc.

- What is the company type?
  - Employer: Files for full-time employment.
  - Non-Employer: No employment associated with the legal entity.
  - Sole Proprietor: No full-time employees.
  - Holding Company: Are legal entities with no economic activities.
- Does the company file its employment data with the US Dept. of Labor?
- Does the company file it benefit plans with the USDOL?
- Verify client reported revenue & industry vs BQ's filings.

Companies should be verified for watch lists such as terrorist watch lists, IRS Income Tax liens, lawsuits, and other liens including bankruptcy. Understanding the size of company revenues and headcounts will provide an understanding of how large a company really is and its available resources.

Summary: Companies that file regularly with government agencies are more easily verified than companies that don't, and as a result, are less likely to engage in fraud. Holding companies that are not economically active may be more likely to commit fraud.

Ideal Business Persona: Make sure companies are registered legal entities, who have full-time employees and have a commercial address. Companies that reside in a residential address, have no employees, or record of economic activity may be legitimate but should require greater verification.

In addition to providing fraud indicators, BQ has developed the **BQ Fraud Score** which numerically defines the number of fraud indicators triggered as a percentage of all indicator fields. This percentage or score can be used to filter out potentially weaker companies for engaging in the lead qualification and sales process, or engaging in various contracts.

National Association of Credit Management (NACM) is a national organization of business-to-business credit managers. NACM was founded in 1896 to promote good laws for sound credit, protect businesses against fraudulent debtors, improve the interchange of credit information, develop better credit practices and methods, and establish a code of ethics. NACM is a member-owned association that exists primarily to serve and support its members, including by representing business credit grantors in all industries and enhancing, promoting, and protecting the interests of business credit and financial management.

BrightQuery is the leading expert in sourcing, organizing, and analyzing government-filed company and employment data. BQ updates all 93 million legal entities and all active 42 million US public & private companies monthly. BrightQuery is the sole provider of historical financials, employment and payroll data for both private & public US companies, sourced from up-to-date validated government filings including up to 1,000 fields per company.