

WHITE PAPER

Modern Approaches to B2B Credit Fraud Prevention in the Nordic Region

From Pattern Recognition to Prevention



Contents

Executive Summary & Introduction	3
The Evolving Fraud Landscape	5
Challenges in Traditional Fraud Detection	7
The Power of Automation and Analytics	9
Automated Decisioning and Signatory Verification	10
Enhancing Trust with Open Accounting and Banking Data	11
The Future of Fraud Preventionin the Nordics	13

Executive Summary & Introduction

B2B credit fraud in the Nordic region has entered a new and more sophisticated phase. Fraud schemes are becoming broader in scale, more embedded within legitimate business activity, and increasingly difficult to detect through traditional methods. Manual processes, fragmented data sources, and outdated verification practices create blind spots that highly organised criminal networks exploit through tactics such as falsified financials, manipulated onboarding, shell companies, and the use of “history companies”.

At the same time, the banking and credit landscape is rapidly evolving. Digital onboarding, accelerated decision cycles, and the growing demand for automation mean that organisations must balance efficiency with heightened risk exposure.

RECENT NORDIC DATA CLEARLY ILLUSTRATES THE URGENCY:

- Sweden identifies fraud risk as one of the most significant threats to the financial sector.¹
- Finland recorded €44M+ in blocked fraud-related transactions in 2024.²
- Norway reported losses of NOK 2.13B, a 150% increase since 2020.³
- Denmark exceeded 15,000 recorded fraud incidents in Q4 2024 alone.⁴

These figures represent only the visible part of the problem. B2B credit fraud often goes unreported and is structurally under-recorded in legal systems, making the true scale significantly larger.

TOP FRAUD RISKS & CHALLENGES IN THE NORDIC MARKET

- 01 Sophisticated corporate structures (e.g., history companies)**
Criminal actors use legitimate company identities and credit histories to bypass onboarding checks.
- 02 Fragmented or unreliable data**
58% of financial institutions distrust their own data, making anomaly detection difficult.
- 03 High reliance on manual workflows**
Around 60% of organisations still rely on manual verification — slow, inconsistent, and vulnerable to manipulation.
- 04 Identity and signatory fraud**
Weak signatory verification exposes companies to impersonation and unauthorised credit actions.
- 05 Manipulated or falsified financial information**
Self-reported data without real-time validation enables fraudsters to present a misleading picture of financial stability.

¹ Bedrägeririsker bland de största hoten mot svenska finans- och försäkringsbolag. November 6, 2025. <https://www.dnb.com/sv-se/nyheter/bedrageririsker-bland-de-storsta-hoten-mot-svenska-finans-och-forsakringsbolag.html>

² Finance Finland, Volume of fraud skyrockets in Finland, February 20, 2025, <https://www.finanssiala.fi/en/news/volume-of-fraud-skyrockets-in-finland-banks-blocked-more-than-e44-millions-worth-of-fraud-related-payments-in-2024/>

³ Svindlet for 2 milliarder kroner. July 8, 2025. <https://www.okokrim.no/svindlet-for-2-milliarder-kroner.6724043-549344.html>

⁴ Statistics Denmark. (2025). Crimes by type and time of offense (2020 Q1 – 2025 Q2): Fraud cases. Dataset retrieved from www.dst.dk

As the digital environment becomes more dynamic, organisations must transition from reactive fraud detection to proactive, data-driven prevention. Modern fraud defence requires a combination of:

- Automation, to ensure consistency and reduce human error
- Analytics, to identify behavioural and financial anomalies
- Verified real-time data, for accurate risk assessment
- Signatory verification, to prevent impersonation and unauthorised authority
- Open Accounting and Open Banking, to reveal the real financial picture behind applications

Nordic businesses — with high digital maturity and strong trust in data-sharing — are uniquely positioned to lead this shift toward integrated, intelligent, and preventative fraud management.

*Unlike consumer fraud, **B2B credit fraud often involves sophisticated schemes** targeting corporate credit systems. Some cases go unreported, which makes it difficult to assess the true scale of the problem.*

FRAUD LOSSES IN NORWAY

Økokrim Estimates 2020–2024

NOK 2.13bn

Lost to fraud in 2024

2020 NOK 0.864 bn

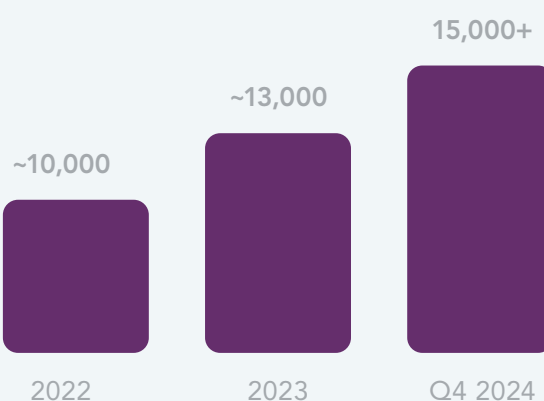
Baseline

2024 NOK 2.13bn

2.5x increase

FRAUD OFFENSES IN DENMARK

Statistics Denmark





The Evolving Fraud Landscape

The Nordic region faces a growing challenge from organised economic crime. In Sweden, authorities estimate that the criminal economy generates between SEK 100 and 150 billion annually¹, with much of this activity remaining unreported. Low risk of detection and high potential profit are the drivers for this growth. Both drivers have significant consequences for the financial system and economic stability.

Economic crime has shifted from isolated offenses to system-threatening structures. Criminal networks establish companies specifically to commit crimes and often layer them within international ownership chains to obscure accountability. Money laundering is at the core of this ecosystem, with front companies, intermediaries, and identity abuse used to legitimise illicit funds.

These operations resemble informal corporate groups. At the top sit parent companies abroad, the middle layer consists of domestic firms with frontmen acting as legal representatives, and at the base are cash-intensive sectors such as construction, restaurants, and healthcare, which serve as channels for moving and cleaning money.

The same structural vulnerabilities exist across the Nordics. In Finland, official data from the Legal Register Centre (Oikeusrekisterikeskus) show that courts resolved more than 6 000 economic-crime cases involving corporate entities in 2024, of which roughly 52 % were classified as fraud or aggravated fraud². Yet there is no specific legal category for credit

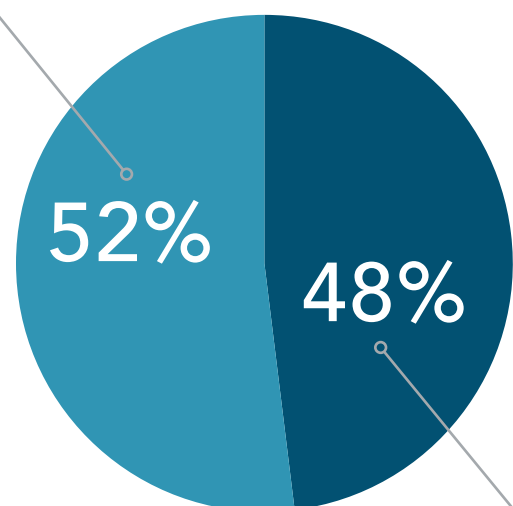
fraud, meaning that B2B credit-related deception is under-recorded.

Common schemes in the B2B space include the use of “history companies” and shell firms with intact credit ratings, falsified financial reports, manipulated supplier-onboarding processes, and fraudulent signatories. These tactics take advantage of weak company checks and inconsistent data controls. Together with light penalties and limited supervision, they create ideal conditions for credit abuse and financial crime.

ECONOMIC CRIME IN FINLAND

Corporate Entity Cases 2024

Fraud & Aggravated Fraud: 3 486 cases



Other Economic Crimes: 3 176 cases

¹ Ekobrottsmyndigheten (2025). Ekobrottsmyndighetens lägesbild maj 2025. Stockholm: Ekobrottsmyndigheten

² Oikeusrekisterikeskus (2025). Economic-crime cases involving corporate entities resolved by Finnish courts, 2024-2025 (dataset). Unpublished data provided to Dun & Bradstreet Nordics (2025).

How “History Companies” Enable Fraud

Around 80 % of criminal networks within the European Union use corporate entities as tools for economic crime.

This following example illustrates how fraudsters exploit legitimate company structures and credit systems:



Company intermediaries sell ready-made firms, either shelf companies (newly formed) or history companies (previously active limited companies with remaining tax IDs and credit ratings).



A criminal actor acquires such a company, installs frontmen on the board, and conceals the real beneficial owner.



Using the firm's credible history, the actor commits fraud, tax evasion, or money-laundering, often applying for credit or grants under false pretences.



When discovered, frontmen are held legally responsible, while the real orchestrators remain hidden. The company is declared bankrupt, leaving debts behind.

Source: “Historikbolag som brottsverktyg,”
Swedish Police, April 2024





Challenges in Traditional Fraud Detection

Traditional approaches to B2B credit fraud detection in the Nordics are increasingly outpaced by the sophistication and scale of modern fraud schemes. Manual processes, fragmented data systems, and outdated verification practices have created blind spots that fraudsters exploit, especially in an environment that is highly digitalised. According to the Financial Services & Insurance Pulse Survey 2025, Swedish financial institutions rank fraud and cyber risk as their top threats, with 77% expressing concern about fraud. Yet despite rising awareness, 23% admit they are not fully prepared to address fraud risks. The most common barriers include lack of clear ownership

or accountability (28%), insufficient leadership support (27%), and regulatory or compliance constraints (27%)¹.

One of the most significant weaknesses lies in data fragmentation. Many credit and risk management systems still operate in silos, where financial data, ownership structures, behavioural signals, and third-party records are stored separately, preventing analysts from identifying cross-pattern anomalies. As the survey shows, 58% of Swedish financial firms distrust their own data, and 55% report data silos that hinder automation and risk analysis². These silos make it nearly impossible to detect subtle yet telltale inconsistencies.

¹ Bedrägeririsker bland de största hoten mot svenska finans- och försäkringsbolag. November 6, 2025.
<https://www.dnb.com/sv-se/nyheter/bedrageririsker-bland-de-storsta-hoten-mot-svenska-finans-och-forsakringsbolag.html>

² Bedrägeririsker bland de största hoten mot svenska finans- och försäkringsbolag. November 6, 2025.
<https://www.dnb.com/sv-se/nyheter/bedrageririsker-bland-de-storsta-hoten-mot-svenska-finans-och-forsakringsbolag.html>

A second key challenge is manual credit assessment workflows. Many Nordic businesses still rely on human-led evaluations to verify company information. This approach is slow, inconsistent, and vulnerable to manipulation. Fraudsters often exploit human error and security gaps to falsify documents, misrepresent authorised signatories, or fabricate company credentials. Key processes (including underwriting, onboarding and risk assessments) remain mostly manual in around 60% of firms.¹ The result is not only financial exposure but also reputational and regulatory risks, particularly in sectors subject to KYC and AML compliance.

Many Nordic businesses still rely on human-led evaluations to verify company information. This approach is slow, inconsistent, and vulnerable to manipulation.

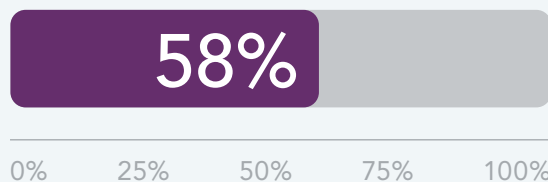
Finally, traditional verification methods fall short in keeping pace with evolving tactics of fraudsters. Fraudsters increasingly combine real and fabricated information to pass legitimacy checks. Without automated systems that connect and analyse data across multiple sources, such entities can maintain clean profiles long enough to commit substantial fraud before being detected.

¹ Bedrägeririsker bland de största hoten mot svenska finans- och försäkringsbolag. November 6, 2025.
<https://www.dnb.com/sv-se/nyheter/bedrageririsker-bland-de-storsta-hoten-mot-svenska-finans-och-forsakringsbolag.html>

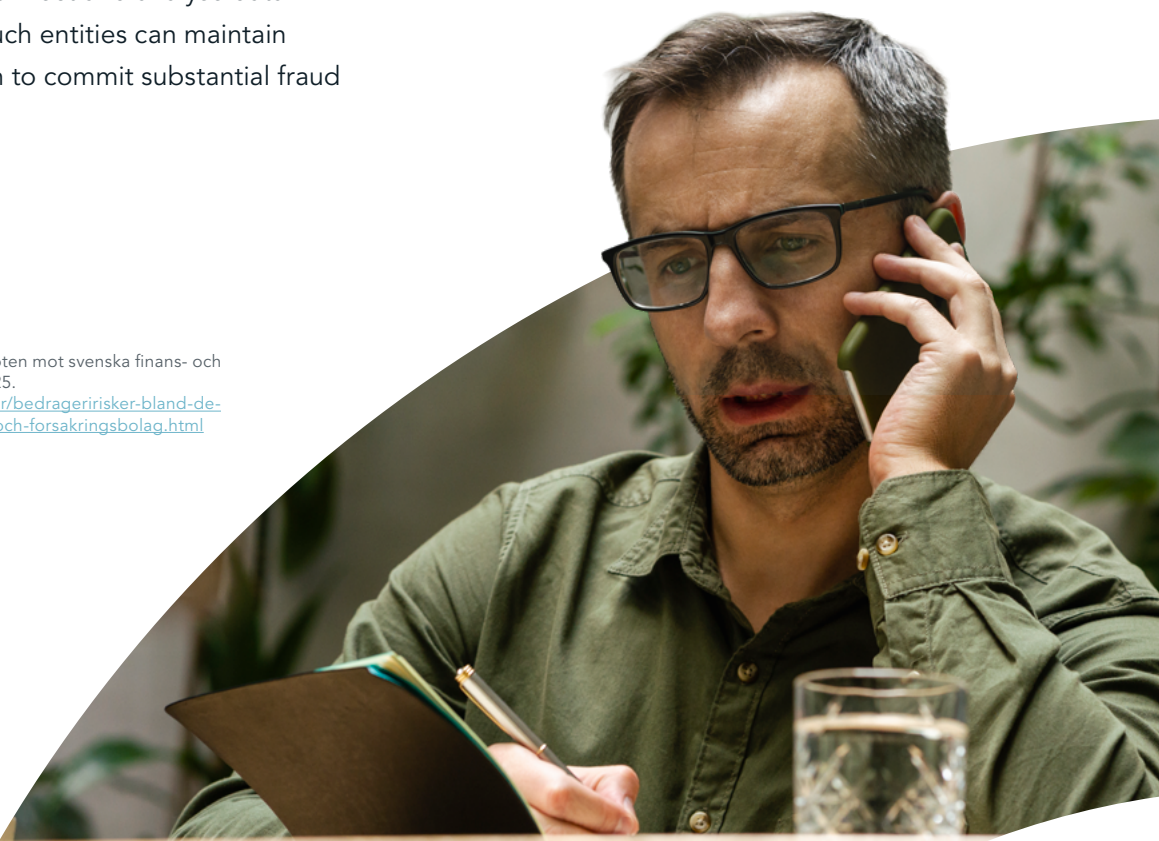
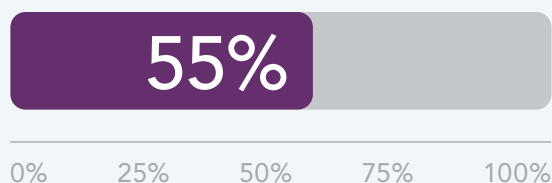
DATA CHALLENGES IN SWEDISH FINANCIAL FIRMS

Survey Results

Distrust Their Own Data



Report Data Silos Hindering Analysis





The Power of Automation and Analytics

As mentioned earlier, the evolution of fraud prevention in the Nordics depends on how well organisations collect, analyse, and act on data. Automation and analytics transform credit and risk management by making decisions faster, more consistent, and evidence based. AI will expand these capabilities, but only when supported by high-quality and well-structured data.

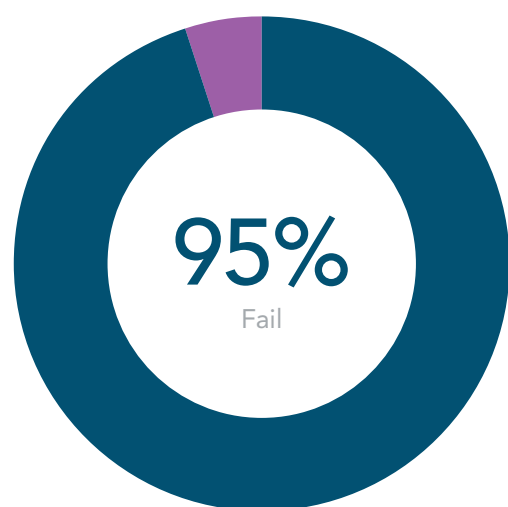
Automation eliminates human error and accelerates workflows. By codifying credit policies into structured processes, companies ensure every decision follows the same principles. One Nordic bank reduced its credit decision time from 35 to 5 minutes, handling seven times more applications without increasing risk. Another organisation onboarding 85 000 suppliers shortened processing from 15 to 2.5 minutes, strengthening both control and compliance.

Analytics provides the intelligence behind these decisions, identifying behavioural and financial anomalies that may signal potential fraud. It also creates the foundation for successful use of AI. Research from MIT¹ shows that 95 % of corporate AI projects fail, not because of technology, but because of poor data quality and weak governance. Reliable, well-structured, and traceable data is therefore the real prerequisite for effective, trustworthy automation and AI.

Together, automation and analytics enable organisations to act faster and smarter while maintaining consistency and control. They also create the foundation for using AI where it truly matters: detecting and combatting fraud. When grounded in high-quality and well-governed data, AI becomes a powerful tool to identify anomalies and ensuring resilience across credit processes.

CORPORATE AI PROJECT SUCCESS RATE

MIT Research



● 95% Failed ● 5% Succeeded

¹ MIT Sloan Management Review & Boston Consulting Group, The State of AI in Business 2023: Winning with AI is Still Hard.



Automated Decisioning and Signatory Verification

Over the past several decades, different industries have accumulated extensive experience in the application of automated processes for credit assessment — spanning both consumer and corporate credits. These systems are typically built upon the credit policies of individual companies and are tailored to the specific characteristics of their industry and target customer segments.

The degree of automation varies depending on the type of credit offered and the geographical markets in which the organization operates. Nonetheless, as a general benchmark, the automation level for corporate credit processes should ideally fall within the range of 70 to 90 percent. This target reflects a strategic ambition to streamline operations and reduce reliance on manual interventions.

The overarching objective is to reserve manual reviews for cases that genuinely warrant deeper scrutiny — such as high-value transactions or applications that trigger alerts related to creditworthiness or potential fraud. By doing so, institutions can enhance operational efficiency while maintaining robust risk controls.

This approach not only supports scalability and consistency in decision-making but also aligns with broader trends in digital transformation and data-driven risk management.

A central part of the automated credit decision process is to ensure that the counterparty has got signing authority. Today, there are good opportunities to incorporate that verification as part of the automated credit assessment process. Understanding who holds signing rights is essential for any business. It ensures that only authorized individuals can make legally binding decisions, sign contracts, and represent the company

in financial or legal matters. But before verifying who has the authority to sign on behalf of the company, it is important to securely identify the counterparty to ensure that it is not a case of identity theft.

This helps reduce the risk of fraud, strengthen accountability, and ensure compliance with corporate governance and legal requirements. An authorized signatory is an individual who has been officially granted the right to sign documents or make decisions on behalf of a company, either individually or jointly.

This designation is typically registered with public authorities and is based on decisions made by the company's board. Authorized signatories may include board members, managers, employees, or even third parties, depending on the company's internal governance and legal structure.

KEY MARKET DRIVERS FOR SIGNATORY DATA ACCESS:



Digital onboarding and efficiency



Fraud prevention and compliance



High adoption of electronic ID



Automation and API integration



Enhancing Trust with Open Accounting and Banking Data

Fraud prevention in B2B credit depends on verifiable trust. Traditional credit assessments often rely on outdated or self-reported data, leaving gaps that fraudsters exploit. Open Accounting and Open Banking help fill those gaps by providing a clear, real-time view of a company's financial health during risk evaluation.

Traditional credit assessments often rely on outdated or self-reported data, leaving gaps that fraudsters exploit.

Open Accounting connects directly to a company's accounting system, providing authorised access to live financial data such as invoices and cash flow.

This allows to spot unusual patterns that could point to falsified financials, like strong reported profits alongside irregular cash flow or overdue bills. It helps improve both fraud prevention and credit accuracy by using verified and up-to-date information.

Open Banking complements this by revealing real liquidity and payment behaviours directly from bank transactions. Accessing this data, under full consent and regulation, helps identify early signs of stress or manipulation that might otherwise go unnoticed.

These capabilities shift credit evaluation from a one-time snapshot to a continuous, real-time process. Having live access to accounting and banking data allows Nordic companies to identify risks earlier, operate more transparently, and build trust between lenders and borrowers based on facts rather than assumptions.



Recommendations for Nordic Businesses

As noted earlier, fraud in the Nordics is evolving in speed, scale, and sophistication. The situation is largely similar across the Nordic countries, and many banks operate throughout the region. But this region also offers unique advantages for prevention with high digitalisation, strong institutional trust, and open-data initiatives. Because of those characteristics, Nordic businesses are particularly well positioned to leverage a multimodal fraud defence.

1

Strengthen verification of business identities and signatories.

Ensure that only authorised representatives can act on behalf of a company. Automated signatory verification reduces impersonation risk and supports compliance with KYC and AML regulations.

2

Use analytics to identify behavioural red flags early.

Monitor for unusual credit activity, sudden changes in management, or inconsistent financial behaviour. Advanced analytics can detect these warning signs before they escalate into losses.

3

Integrate real-time financial data into credit assessments.

Adopt Open Accounting and Open Banking connections to access verified, up-to-date financials rather than relying solely on self-reported statements.

4

Automate decisioning to ensure consistency and efficiency.

Codify credit policies into automated workflows to minimise human error, improve response times, and focus analyst expertise on complex or borderline cases.

5

Collaborate across industries and borders.

Fraud patterns in the Nordics often cross jurisdictions. Sharing data and insights between banks, credit providers, and authorities strengthens early detection and collective defence.

CONCLUSION

The Future of Fraud Prevention in the Nordics

The future of fraud prevention in the Nordics will be defined by integration, data, intelligence, and trust. As automation and data connectivity continue to expand, companies that unify their credit and fraud processes around verified data will gain a significant advantage. Automated decision-making will ensure consistency and speed, analytics will ensure early detection, signatory verification will reduce impersonation and governance risk, and open-data systems will make financial activity visible in real-time.

But technology alone is not enough. Collaboration between lenders, data providers, and public authorities is crucial to share insights and strengthen regional resilience.

Now is the time for Nordic businesses to modernise their fraud prevention frameworks and to replace manual checks with dynamic, data-driven monitoring. Automation needs to shift from a compliance necessity into a strategic defence.

To learn more about implementing automated credit decision-making or fraud-risk solutions, contact your local Dun & Bradstreet representative for a consultation.

CONTACT

Swedish Team ›



CONTACT

Finish Team ›



CONTACT

Danish Team ›



CONTACT

Norwegian Team ›



References

Dun & Bradstreet. (2025). Financial Services & Insurance Pulse Survey 2025.

<https://www.dnb.com/sv-se/nyheter/bedrageririsker-bland-de-storsta-hoten-mot-svenska-finans-och-forsakringsbolag.html>

Finance Finland. (2025, February 20). Volume of fraud skyrockets in Finland: Banks blocked more than €44 million worth of fraud-related payments in 2024. Retrieved from <https://www.finanssiala.fi/en/news/volume-of-fraud-skyrockets-in-finland-banks-blocked-more-than-e44-millions-worth-of-fraud-related-payments-in-2024/>

Statistics Denmark. (2025). Crimes by type and time of offense (2020 Q1 – 2025 Q2): Fraud cases [Dataset]. Retrieved from www.dst.dk

Ekobrottsmyndigheten. (2025). Ekobrottsmyndighetens lägesbild maj 2025. Stockholm: Ekobrottsmyndigheten.

Oikeusrekisterikeskus. (2025). Economic-crime cases involving corporate entities resolved by Finnish courts, 2024–2025 [Unpublished dataset]. Provided to Dun & Bradstreet Nordics.

Swedish Police. (2024, April). Historikbolag som brottsverktyg.

MIT Sloan Management Review & Boston Consulting Group. (2023). The State of AI in Business 2023: Winning with AI is Still Hard.

Økokrim (2025, July). Svindlet for 2 milliarder kroner. <https://www.okokrim.no/svindlet-for-2-milliarder-kroner.6724043-549344.html>



ABOUT DUN & BRADSTREET®

Dun & Bradstreet, a leading global provider of B2B data, insights and AI-driven platforms, helps organizations around the world grow and thrive. Dun & Bradstreet's Data Cloud fuels solutions and delivers insights that empower customers to grow revenue, increase margins, manage risk, and help stay compliant — even in changing times. Since 1841, companies of every size have relied on Dun & Bradstreet.

The information provided is for suggestion purposes only and is based on best practices. Dun & Bradstreet is not liable for the outcome or results of specific programs or tactics undertaken based on your use of the information. Please contact an attorney or tax professional if you are in need of legal or tax advice.

© Dun & Bradstreet, Inc. 2026. All rights reserved. (CAM-442 5/26)

dnb.com