

Protecting Your Bottom Line: Identifying and Preventing Fraud in Commercial Credit Transactions

BERNSTEIN ■ BURKLEY
ATTORNEYS AT LAW

A business approach to legal service SM

Presented by
Shawn P. McClure, Esq. Bernstein-Burkley, P.C.
smcclure@bernsteinlaw.com

Introduction

Objective: To equip credit managers with the tools and knowledge to identify, prevent, and respond to commercial credit fraud.

Why This Matters:

- Rising sophistication of fraud schemes.
- Increased exposure in fast-paced commercial environments.
- Significant financial and reputational losses at stake.

Evolving Fraud Landscape

Trends in Commercial Credit Fraud:

- Synthetic Business Identity Fraud – Blending real and fictitious information.
- Business Email Compromise Fraud – Cyberattacks that infiltrate or spoof email systems.
- Account Takeover Fraud – Credential phishing, malware, or third-party data breaches.
- Trade Credit Fraud Using Supply Chain Disruption – Supply chain volatility used by hackers to exploit urgency and strained verification processes.

Evolving Fraud Landscape

Trends in Commercial Credit Fraud:

- First Party Business Fraud - Real businesses misrepresenting financial information to obtain credit they can't or won't pay back.
- Buy Now Pay Later Abuse – Options for business-to-business BNPL are growing. Fraud can go undetected for a period of time.
- Insider Collusion – Employees motivated by economic pressure, bribery, or shared criminal intent. Certain business more susceptible than others.

Evolving Fraud Landscape

Trends in Commercial Credit Fraud:

- AI – Powered Fraud Schemes – AI works both ways. Fraudsters can increase scale and believability of fraud schemes.
- Cross-Border Credit Fraud – Foreign shell companies and/or intermediaries obscure the real parties.
- Regulatory Arbitrage and Compliance Loopholes – Targeting under-regulated or high-volume sectors.

Impact of Fraud

Impact on Businesses

- Financial Losses – Direct loss, write-offs, and increased costs.
- Cash Flow Disruption – Impact on other areas of business.
- Operational Disruption – Time and resources are diverted. Delay of projects, slow customer response times, and increase employee workloads.

Impact of Fraud

Impact on Businesses

- Legal and Compliance Exposure – Potential lawsuits if fraud implicates clients, partners, or cause third-party losses. Internal controls violating industry standards.
- Reputational Damage – Loss of business, reduced trust, and difficulty securing future partnerships.
- Insurance Complications – Cyber policies may cover, but not all losses are insurable. Impact on future premiums.

Key Fraud Risk Indicators

Red Flags to Watch:

- Business Identity Concerns
 - Newly formed entities with high credit limit applications.
 - Inconsistent or unverifiable business registration details.
 - Mismatched EIN, business names, address, etc. across documents.
- Application Concerns
 - Pressure to expedite approval.
 - Use of free email domains versus corporate domains.
 - Both incomplete and overly polished financial statements.
 - Unverifiable information (trade references and websites).

Key Fraud Risk Indicators

Red Flags to Watch:

- Suspicious Financial Behavior
 - Sudden increase in credit usage or requests to raise credit limits.
 - Repeated late payments followed by large unexpected payments.
 - Rapid expansion in purchase activity without matching revenue increase.
- Digital Red Flags
 - IP address geolocation doesn't match company's physical address.
 - Use of VPN or anonymized browsing during application or login.
 - Multiple businesses using the same contact information or address.

Key Fraud Risk Indicators

Red Flags to Watch:

- Account Takeover Indicators
 - Unusual login times or geographies.
 - Changes in contact info followed by large credit transactions.
 - Requests for wire transfers or changes in ACH instructions from unfamiliar parties.
- Behavioral Red Flags
 - Applicant avoids standard processes or due diligence.
 - Aggressive pushback on verification steps.
 - Refusal to provide key documents like bank statements or tax returns.

Prevention Strategies

- Strengthen Business Verification
 - Third-party business verification tools (e.g. Dun & Bradstreet, LexisNexis, Experian Business).
 - Confirm EINs directly via IRS records.
 - Conduct reversal lookups on phone numbers and emails.
- Leverage AI/ML for Anomaly Detection
 - Machine Learning Models to flag unusual behavior patterns in:
 - Spending.
 - Credit Utilization.
 - Login/IP Behavior.

Prevention Strategies

- Require Multi-Factor Authentication (MFA)
 - Apply MFA for both customer portals and internal systems.
 - A must for access to sensitive financial data or credit lines.
- Conduct Manual Reviews for High-Risk Accounts
 - Flag accounts with rapid growth or large credit line increases for additional scrutiny.
 - Human reviewers to validate supporting documents like invoices, PO history, and vendor lists.
- Monitor Public Records and News Sources
 - Set alerts on key clients or borrowers for bankruptcy filings, lawsuits, or negative news.

Prevention Strategies

- Secure Internal Systems
 - Train staff on recognizing phishing and social engineering.
 - Segregate duties and monitor employee access to prevent insider fraud.
- Establish Fraud Response Protocols
 - Create clear escalation paths for suspected fraud cases.
 - Keep a legal and investigative playbook ready for containment and reporting.

Collaborative Defense

- Partnering Across Departments
 - Finance.
 - Compliance.
 - Legal.
 - Sales.
- External Collaboration
 - Industry networks.
 - Credit bureaus.
 - Law Enforcement.
- Information Sharing and Communication.

Suspected Fraud

- Immediate Steps
 - Isolate and document the incident.
 - Notify all internal stakeholders.
 - Escalate to legal/compliance team.
- Post-Incident Review
 - Root cause analysis.
 - Control enhancements.
 - Employee retraining if needed.

Conclusion & Key Takeaways

- Fraud is evolving – so must your defenses.
- Early detection hinges on vigilance and good processes.
- Prevention is a shared responsibility.
- Technology + training = effective protection.
- Stay informed and proactive.



Creditors' Rights

Shawn P. McClure

Partner

Licensed in PA, OH, and WV

Thank you

EMAIL

smcclure@bernsteinlaw.com

PHONE

412-456-8117

OFFICE ADDRESS

601 Grant Street, 9th Floor, Pittsburgh, PA 15219