

Guarding Against Deception



Understanding fraud and best practices.

Presented by: Amy L Cook CCE

2025 B2B Credit & Payment Fraud Trends and Stats

- U.S. companies lost an average of **9.8% of their equivalent annual revenue** to fraud in 2025, a significant increase from previous years.
- Direct fraud losses exceeded **\$1 million** for nearly one-third of financial institutions.
- **47% of credit managers** cite fraud as the single biggest barrier to expanding online B2B sales.
- **38% of professionals** report detecting fraud attempts at least once per quarter.
- **12% of businesses** face fraud attempts on a weekly basis.

IN THE NEXT BUSINESS HOUR (2025 US EST.)...



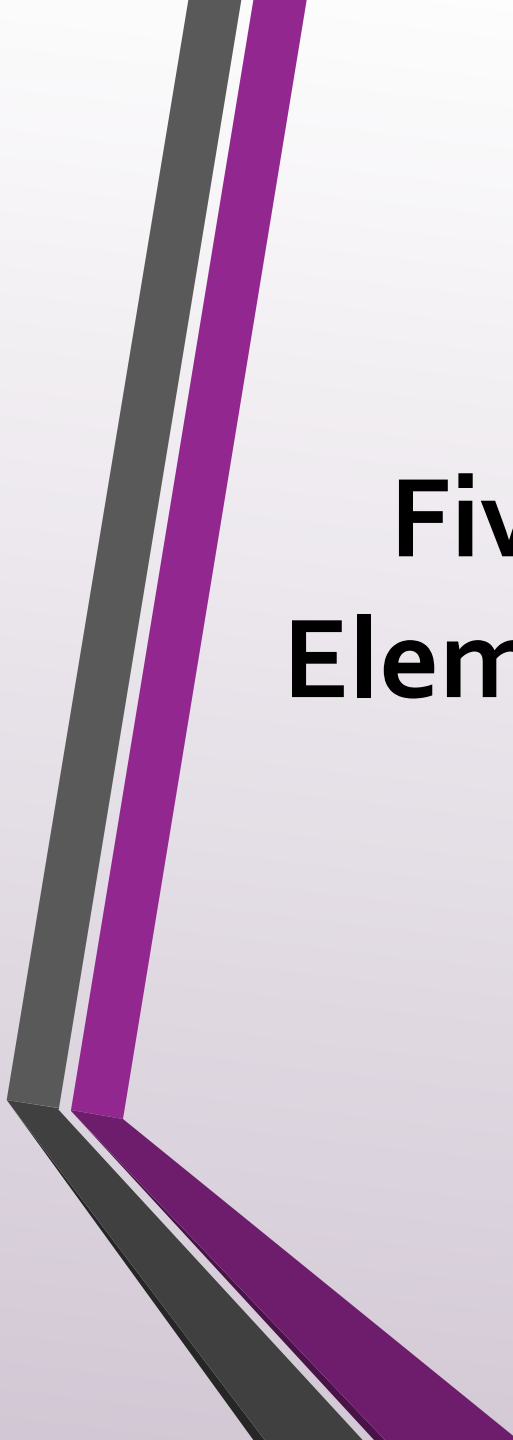
IN THE NEXT YEAR...

2.5% of business
names will
change

1.2% of telephone
numbers
will change

1.5% of CEOs
will change

How do we keep up?



Five Basic Elements of Fraud

False Representation: This means making a false statement or omitting a material fact that should have been disclosed.

Knowledge of Falsity: The person making the false representation must know or believe that the statement is false or misleading.

Intent to Deceive: The person must intend for the other party to rely on the false representation.

Justifiable Reliance: The victim must have relied on the false representation, and that reliance must have been reasonable.

Damages: The victim must have suffered actual damages as a result of their reliance on the false representation.



Common Types of Fraud

- Fraudulent Credit Application
- Purchase Order Fraud
- Overordering and reselling
- Identity theft or misrepresentation
- Payment Method Fraud
- Dispute Fraud

Red Flags and Warning Signs

- **Discrepancies in Customer Information**
 - Multiple accounts with slight variations in the same name or other information (e.g., William Smith, Will Ian Smith).
 - Different customers/orders using the same contact information.
 - Accounts with unvalidated or inconsistent information
- **Speed – need it now**
- **Transactions Inconsistent with Customer Profiles**
 - Transactions/orders that don't match the customer's typical habits, change in behavior
 - Payments or received funds that don't align with the customers habits or known abilities



Preventative Measures

1. Strong Internal Controls

- Segregation of Duties
- Access Controls

2. Employee Training and Awareness

- Regular Training
- Fraud Awareness Programs

3. Robust Verification Processes

- Customer Verification
- Transaction Monitoring

Preventative Measures

4. Use of Technology

- Artificial Intelligence and Machine Learning
- Encryption and Access Controls

5. Regular Audits and Reviews

- Internal Audits
- External Audits

6. Fraud Detection Tools

- Transaction Monitoring Systems
- Geolocation and IP Tracking



- **Your awareness is the strongest shield.** Technology can block the known, but your intuition and action can stop the deceptive.
- **Trust Your Gut:** If a request feels wrong, it probably is.
- **Own the Pause:** Speed is the fraudster's tool; diligence is ours.
- **Protect the Mission:** We don't just guard data; we guard our reputation and our future.