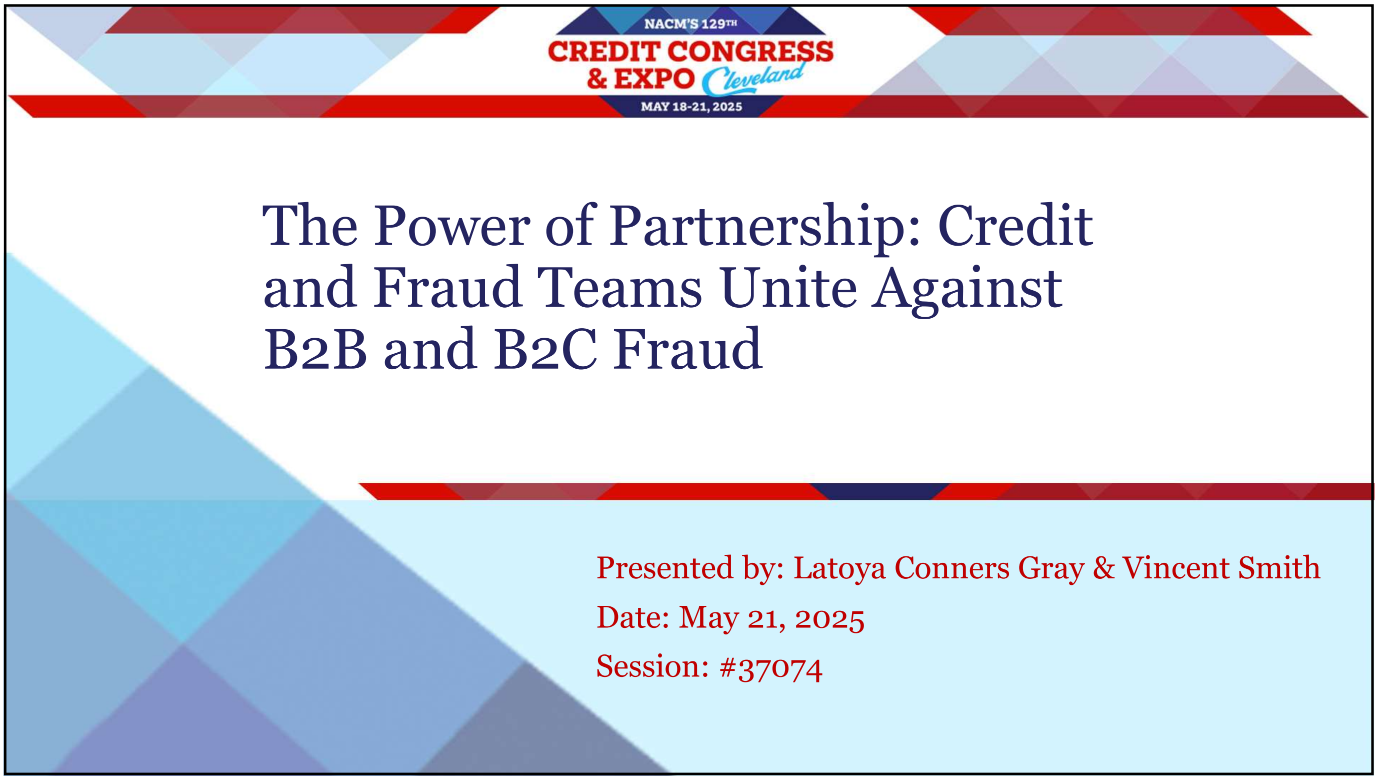


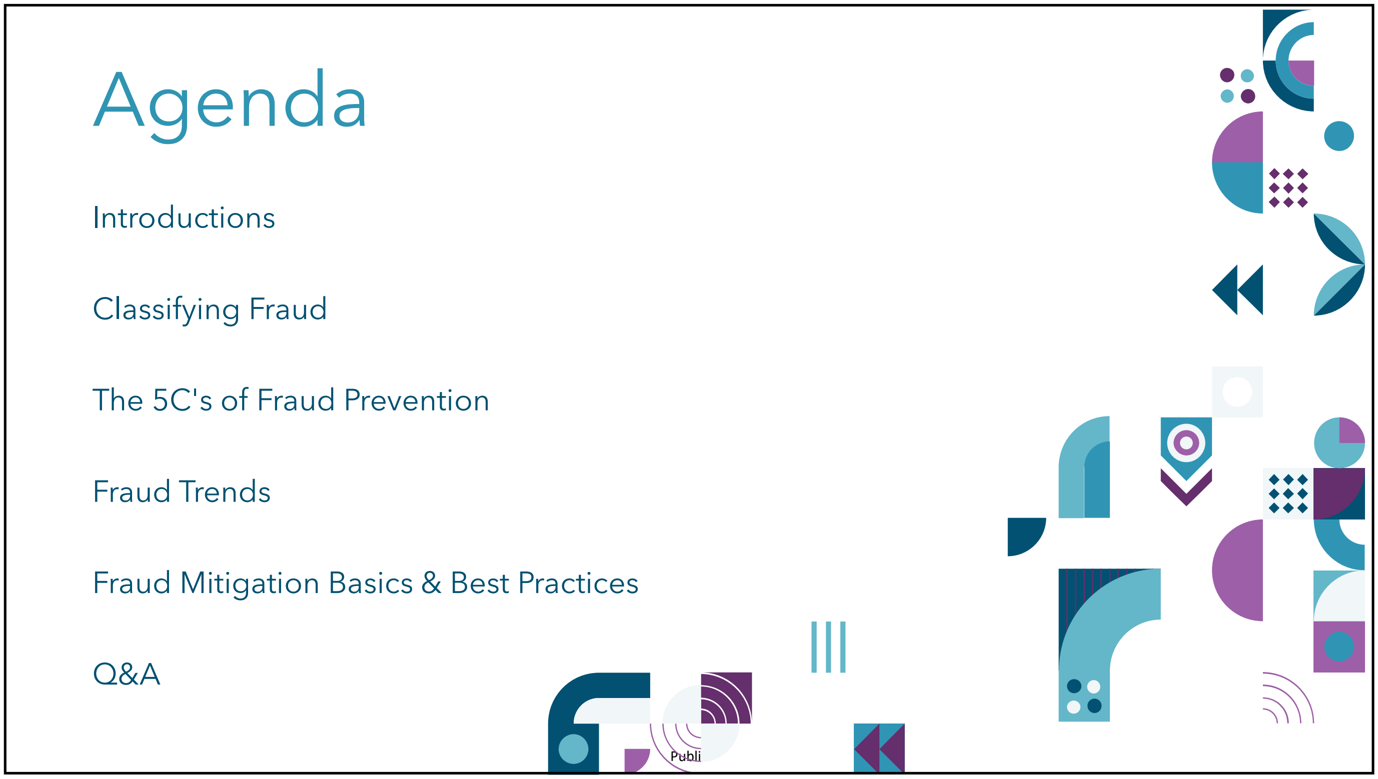
NACM'S 129TH CREDIT CONGRESS & EXPO Cleveland MAY 18-21, 2025

The Power of Partnership: Credit and Fraud Teams Unite Against B2B and B2C Fraud

Presented by: Latoya Conners Gray & Vincent Smith

Date: May 21, 2025

Session: #37074



Agenda

Introductions

Classifying Fraud

The 5C's of Fraud Prevention

Fraud Trends

Fraud Mitigation Basics & Best Practices

Q&A

Publi

About Us

Latoya Conners Gray

Senior Director, Credit, Fraud, and Risk Mgmt.

GRAINGER

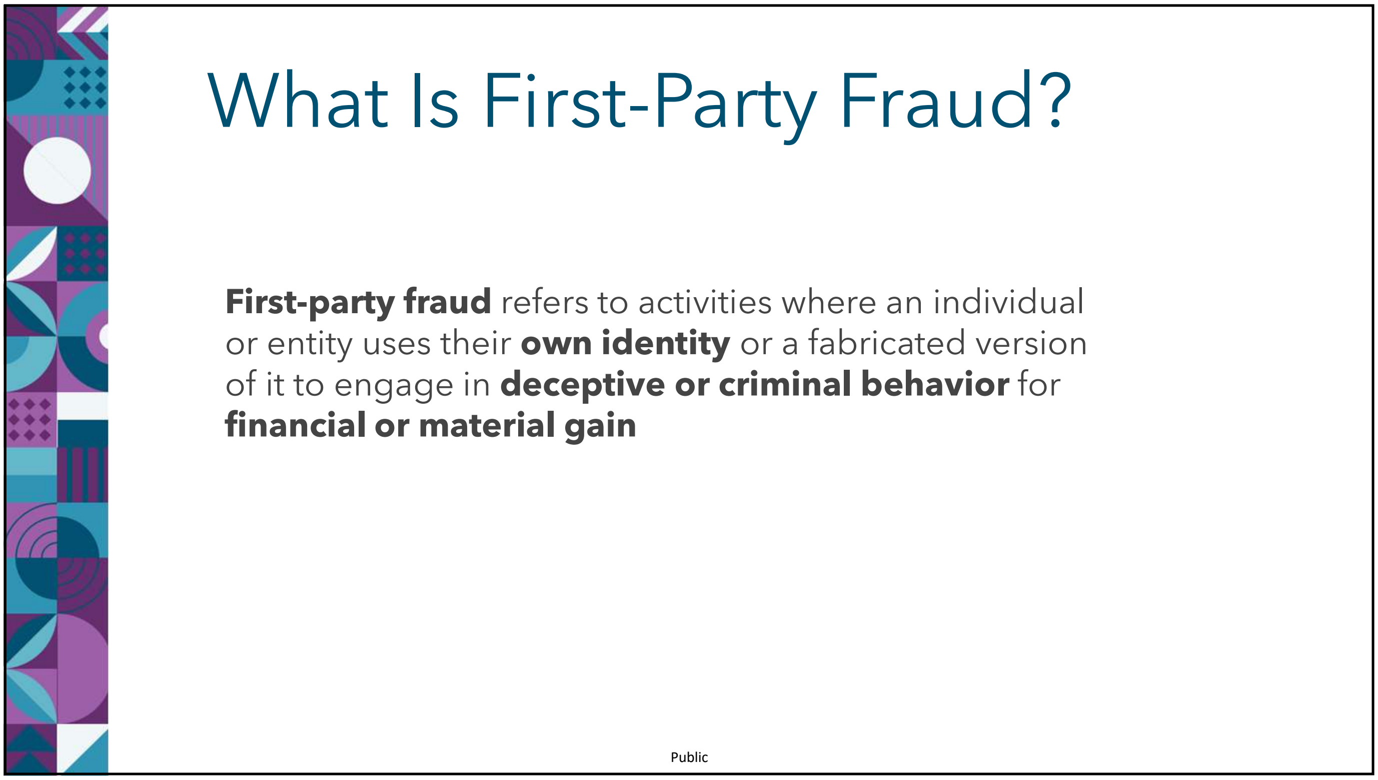
Vincent Smith

Senior Principal, Fraud Product Mgmt.

dun & bradstreet

Public

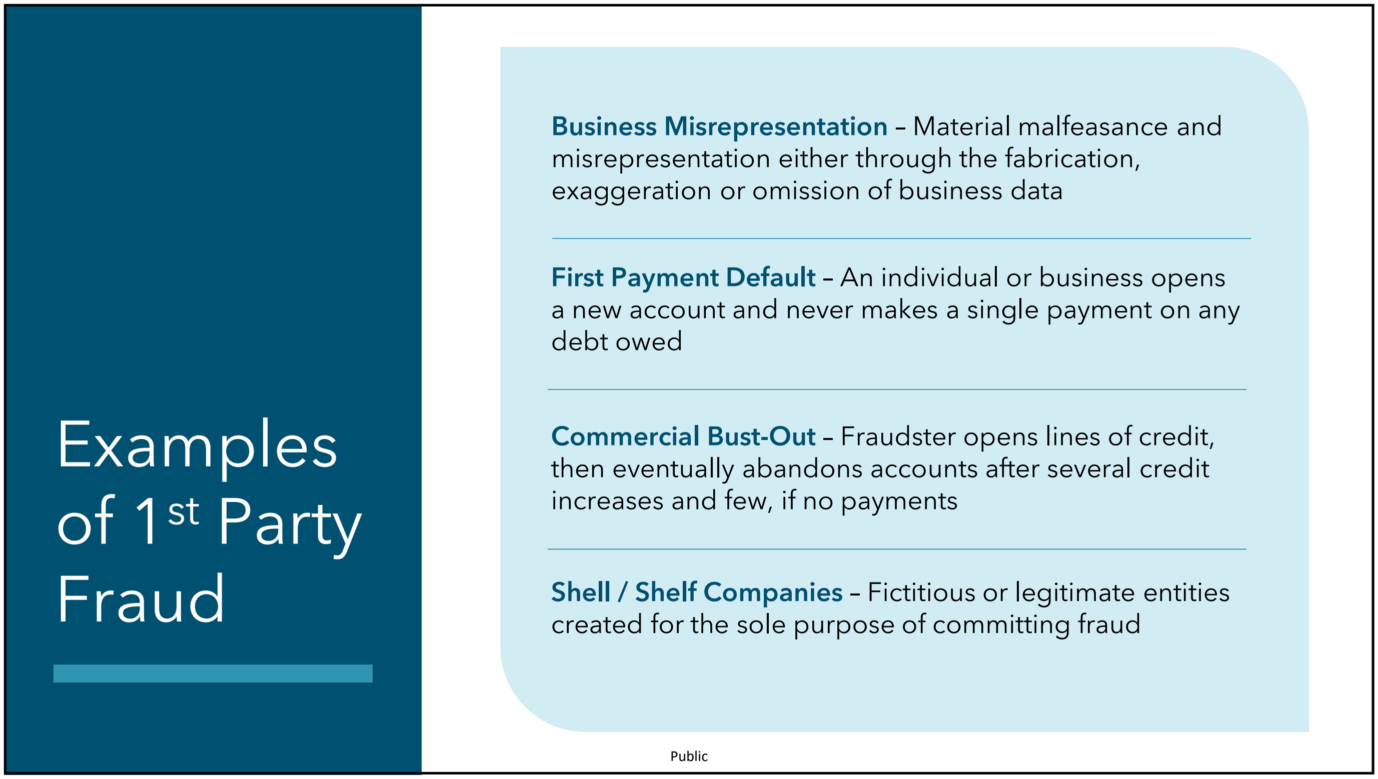
Classifying Fraud



What Is First-Party Fraud?

First-party fraud refers to activities where an individual or entity uses their **own identity** or a fabricated version of it to engage in **deceptive or criminal behavior** for **financial or material gain**

Public



Examples of 1st Party Fraud

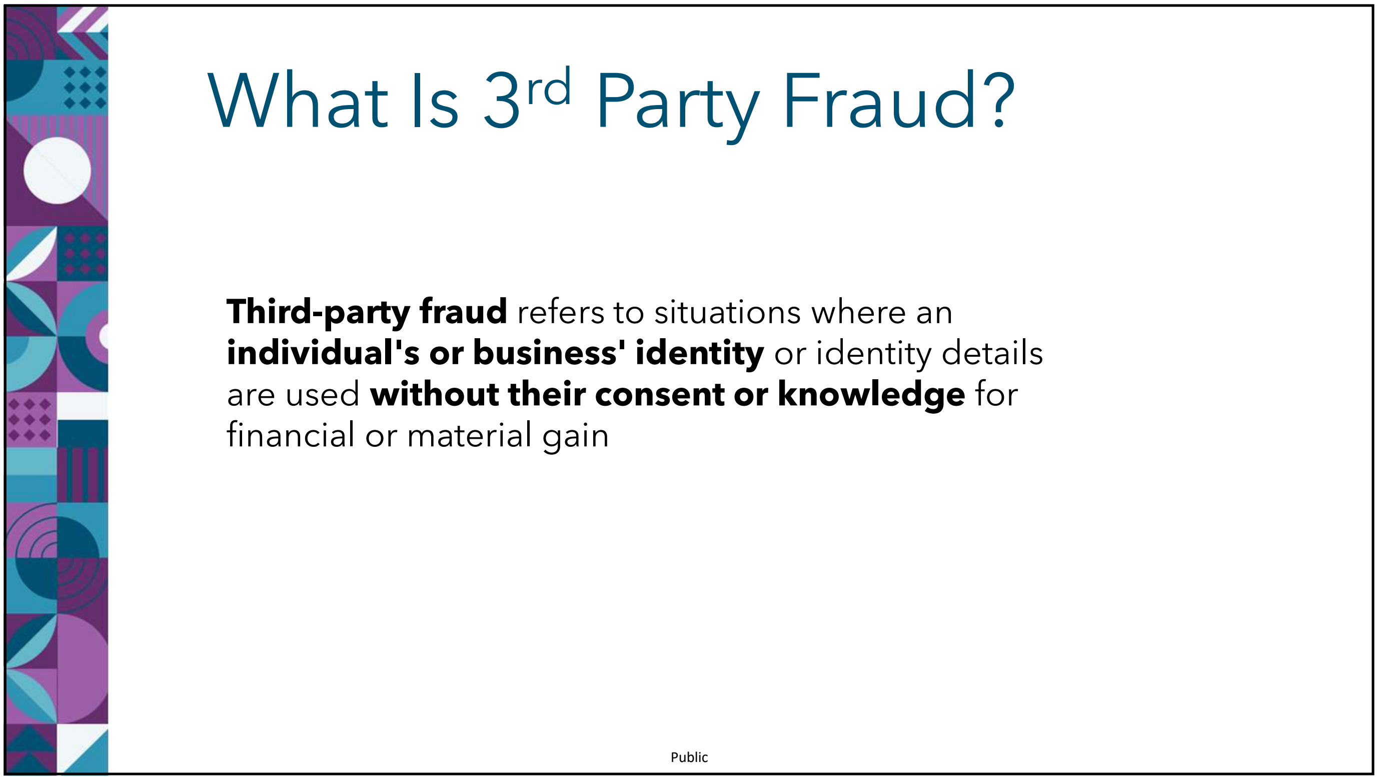
Business Misrepresentation – Material malfeasance and misrepresentation either through the fabrication, exaggeration or omission of business data

First Payment Default – An individual or business opens a new account and never makes a single payment on any debt owed

Commercial Bust-Out – Fraudster opens lines of credit, then eventually abandons accounts after several credit increases and few, if no payments

Shell / Shelf Companies – Fictitious or legitimate entities created for the sole purpose of committing fraud

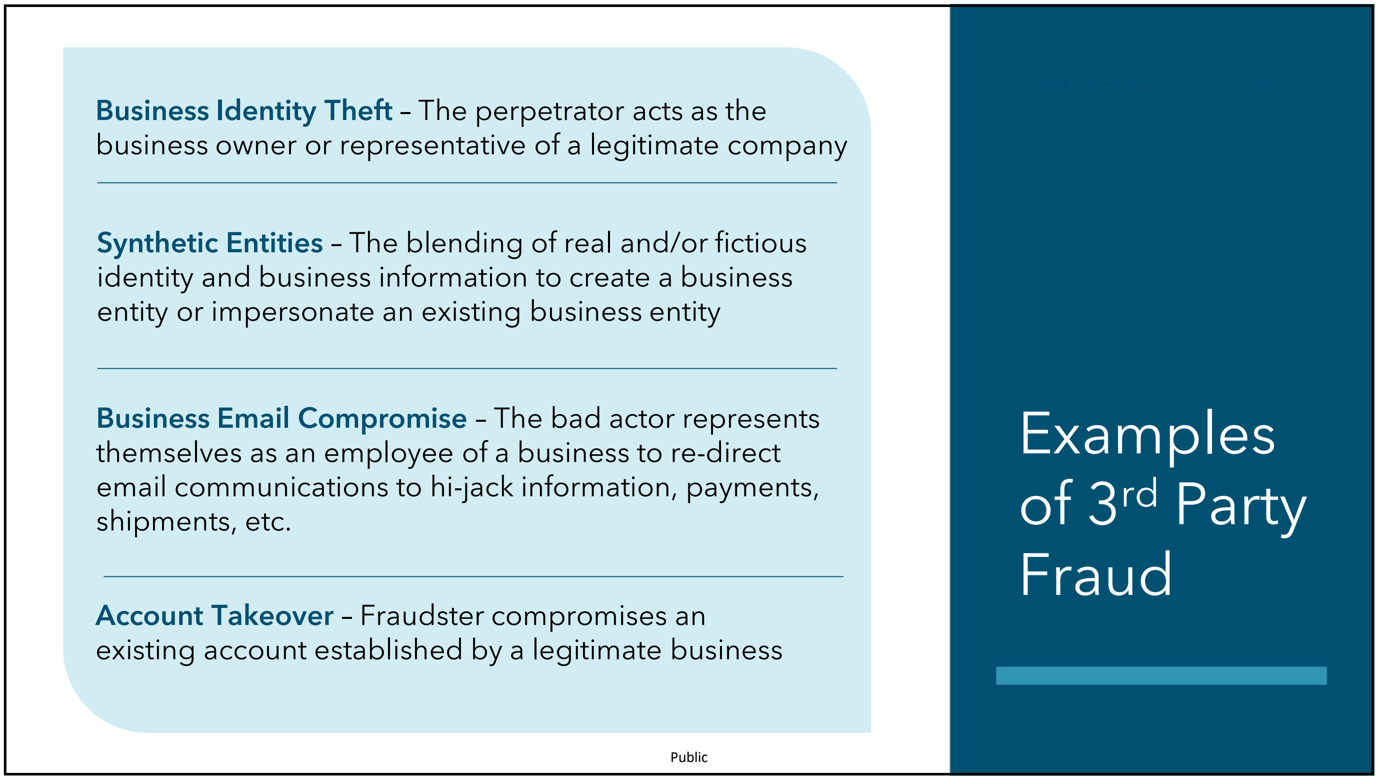
Public



What Is 3rd Party Fraud?

Third-party fraud refers to situations where an **individual's or business' identity** or identity details are used **without their consent or knowledge** for financial or material gain

Public



Examples of 3rd Party Fraud

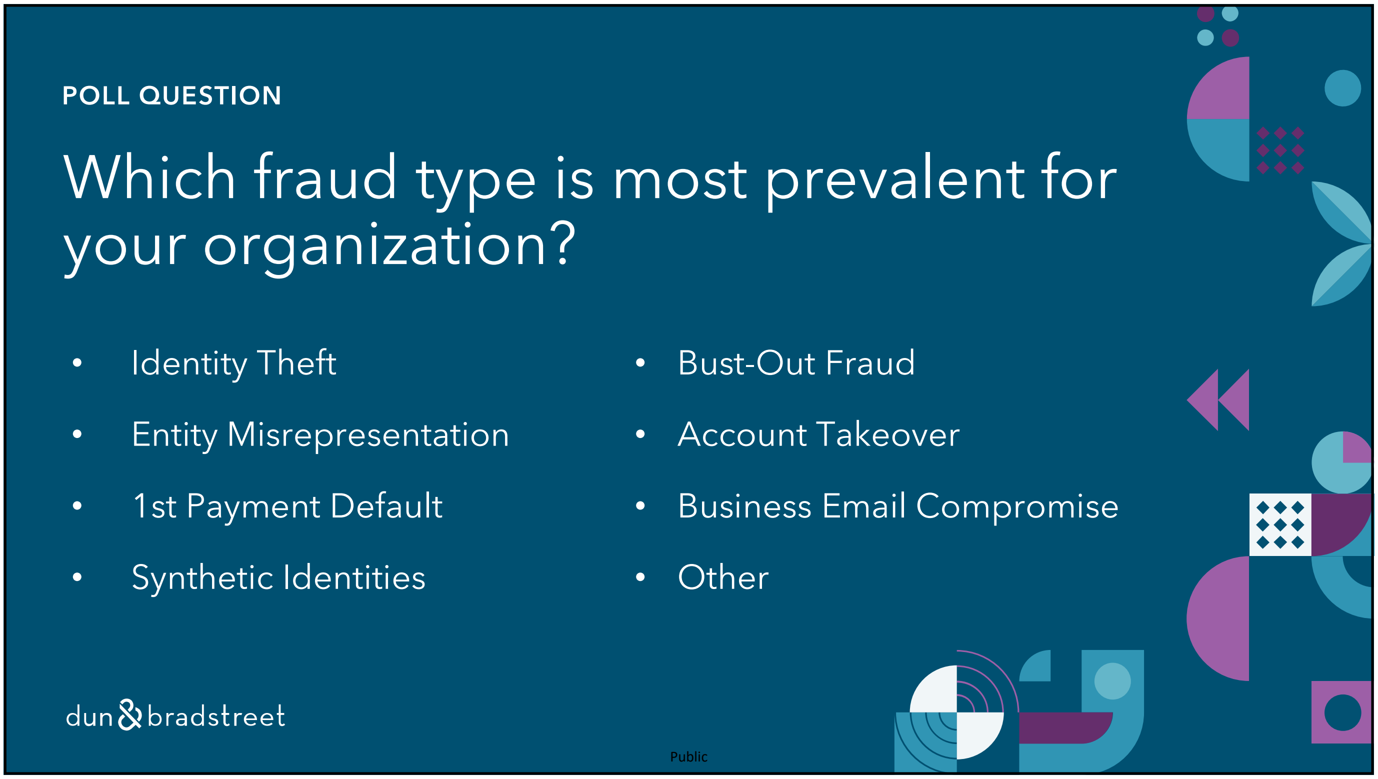
Business Identity Theft – The perpetrator acts as the business owner or representative of a legitimate company

Synthetic Entities – The blending of real and/or fictious identity and business information to create a business entity or impersonate an existing business entity

Business Email Compromise – The bad actor represents themselves as an employee of a business to re-direct email communications to hi-jack information, payments, shipments, etc.

Account Takeover – Fraudster compromises an existing account established by a legitimate business

Public



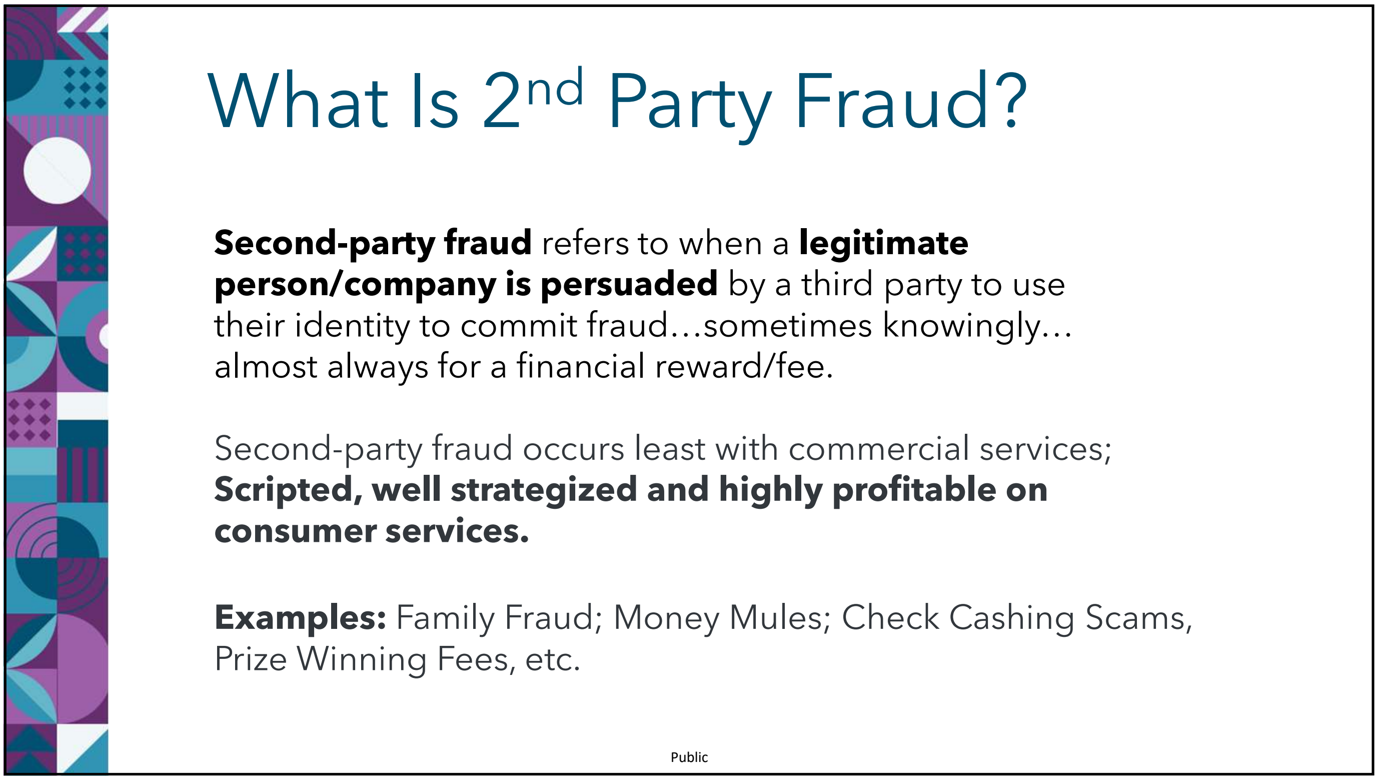
POLL QUESTION

Which fraud type is most prevalent for your organization?

- Identity Theft
- Entity Misrepresentation
- 1st Payment Default
- Synthetic Identities
- Bust-Out Fraud
- Account Takeover
- Business Email Compromise
- Other

dun & bradstreet

Public



What Is 2nd Party Fraud?

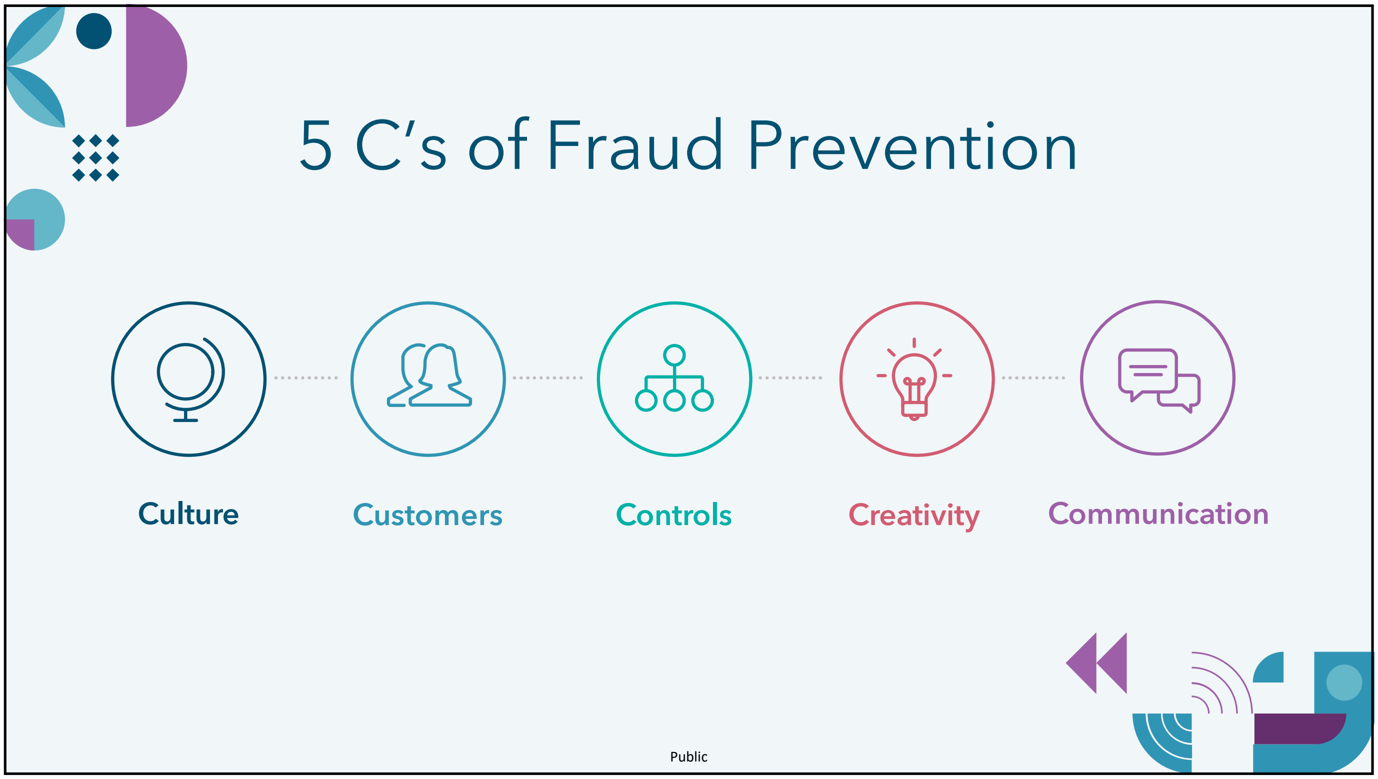
Second-party fraud refers to when a **legitimate person/company is persuaded** by a third party to use their identity to commit fraud…sometimes knowingly…almost always for a financial reward/fee.

Second-party fraud occurs least with commercial services; **Scripted, well strategized and highly profitable on consumer services.**

Examples: Family Fraud; Money Mules; Check Cashing Scams, Prize Winning Fees, etc.

Public

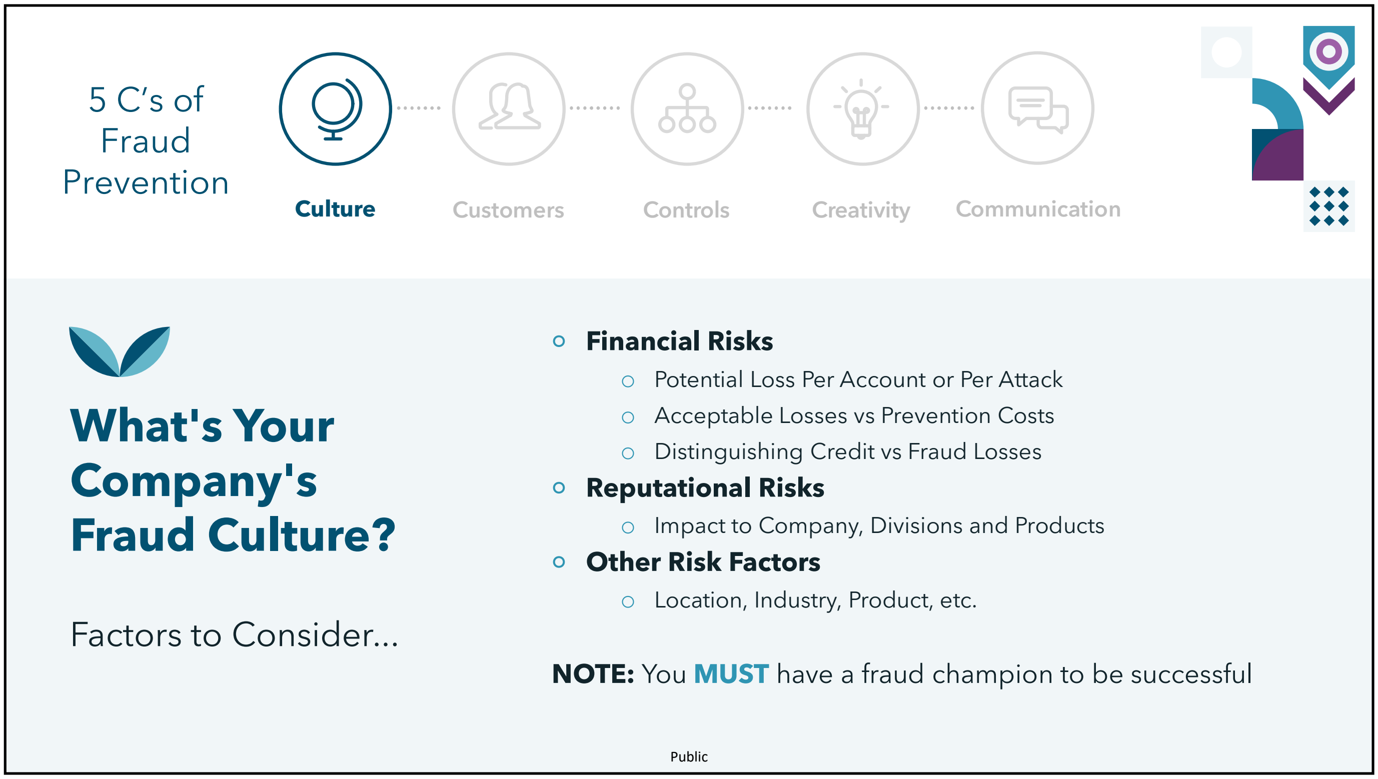
The 5 C’s of Fraud Prevention



5 C’s of Fraud Prevention

- Culture
- Customers
- Controls
- Creativity
- Communication

Public



5 C's of Fraud Prevention

Culture Customers Controls Creativity Communication

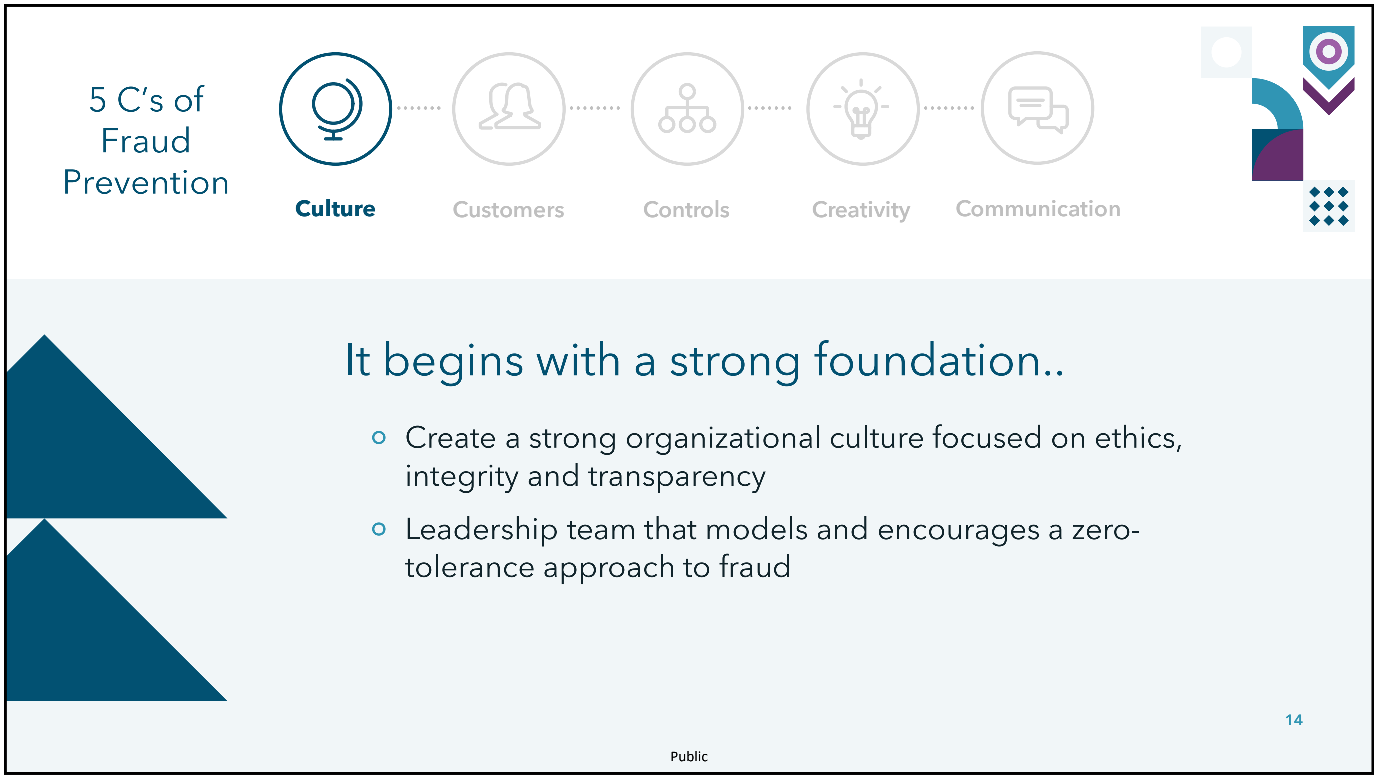
What's Your Company's Fraud Culture?

Factors to Consider...

- **Financial Risks**
  - Potential Loss Per Account or Per Attack
  - Acceptable Losses vs Prevention Costs
  - Distinguishing Credit vs Fraud Losses
- **Reputational Risks**
  - Impact to Company, Divisions and Products
- **Other Risk Factors**
  - Location, Industry, Product, etc.

NOTE: You **MUST** have a fraud champion to be successful

Public



5 C's of Fraud Prevention

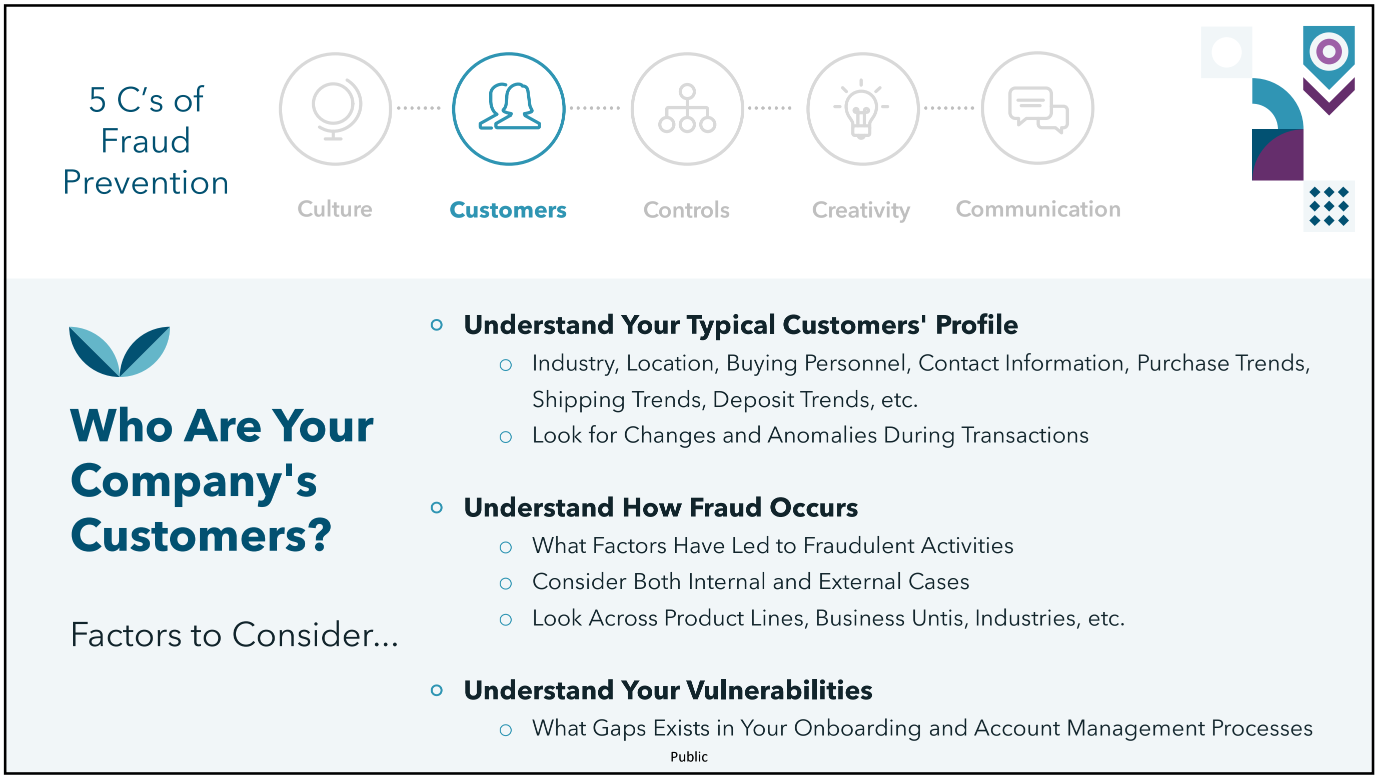
Culture Customers Controls Creativity Communication

It begins with a strong foundation..

- Create a strong organizational culture focused on ethics, integrity and transparency
- Leadership team that models and encourages a zero-tolerance approach to fraud

14

Public



5 C's of Fraud Prevention

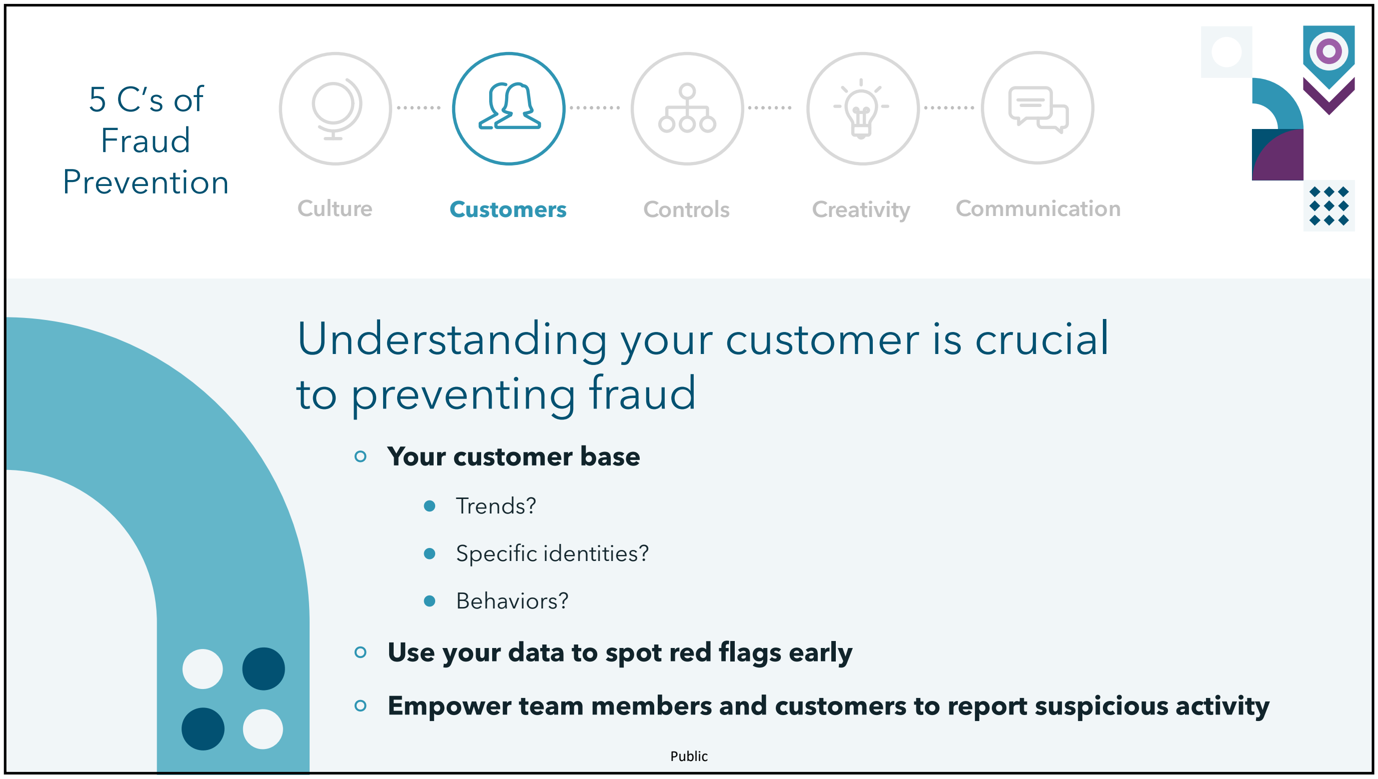
Culture · **Customers** · Controls · Creativity · Communication

Who Are Your Company's Customers?

Factors to Consider…

- **Understand Your Typical Customers' Profile**
  - Industry, Location, Buying Personnel, Contact Information, Purchase Trends, Shipping Trends, Deposit Trends, etc.
  - Look for Changes and Anomalies During Transactions
- **Understand How Fraud Occurs**
  - What Factors Have Led to Fraudulent Activities
  - Consider Both Internal and External Cases
  - Look Across Product Lines, Business Untis, Industries, etc.
- **Understand Your Vulnerabilities**
  - What Gaps Exists in Your Onboarding and Account Management Processes

Public



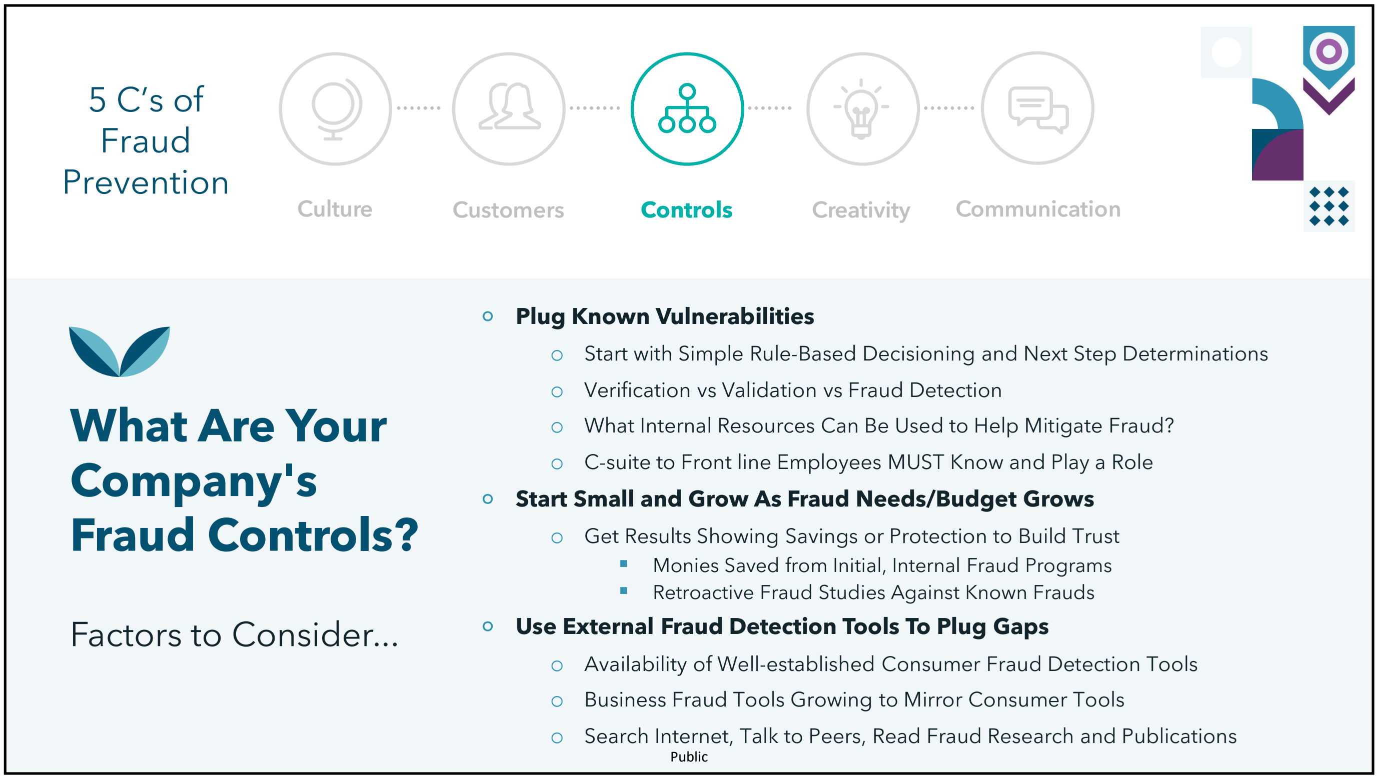
5 C's of Fraud Prevention

Culture · **Customers** · Controls · Creativity · Communication

Understanding your customer is crucial to preventing fraud

- **Your customer base**
  - Trends?
  - Specific identities?
  - Behaviors?
- **Use your data to spot red flags early**
- **Empower team members and customers to report suspicious activity**

Public



5 C's of Fraud Prevention

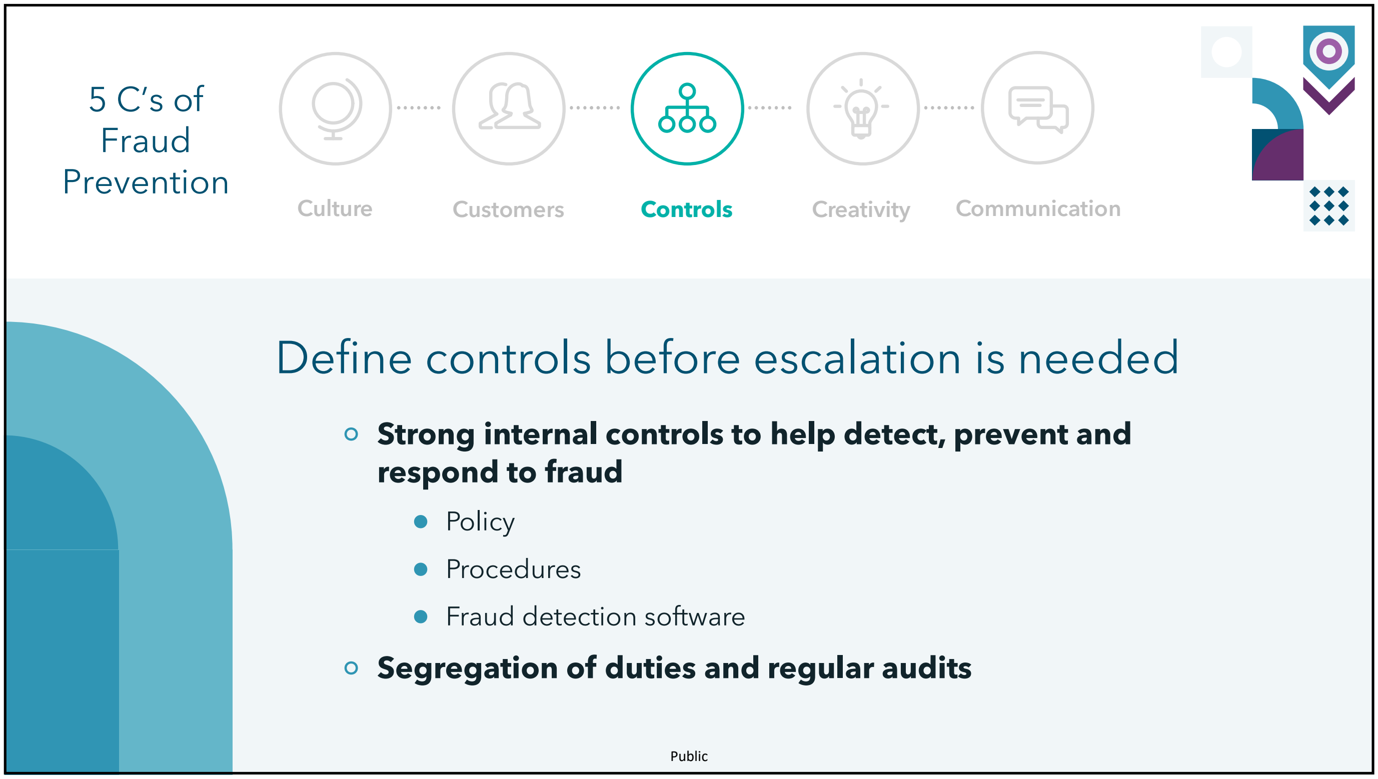
Culture · Customers · **Controls** · Creativity · Communication

What Are Your Company's Fraud Controls?

Factors to Consider...

- **Plug Known Vulnerabilities**
  - Start with Simple Rule-Based Decisioning and Next Step Determinations
  - Verification vs Validation vs Fraud Detection
  - What Internal Resources Can Be Used to Help Mitigate Fraud?
  - C-suite to Front line Employees MUST Know and Play a Role
- **Start Small and Grow As Fraud Needs/Budget Grows**
  - Get Results Showing Savings or Protection to Build Trust
    - Monies Saved from Initial, Internal Fraud Programs
    - Retroactive Fraud Studies Against Known Frauds
- **Use External Fraud Detection Tools To Plug Gaps**
  - Availability of Well-established Consumer Fraud Detection Tools
  - Business Fraud Tools Growing to Mirror Consumer Tools
  - Search Internet, Talk to Peers, Read Fraud Research and Publications

Public



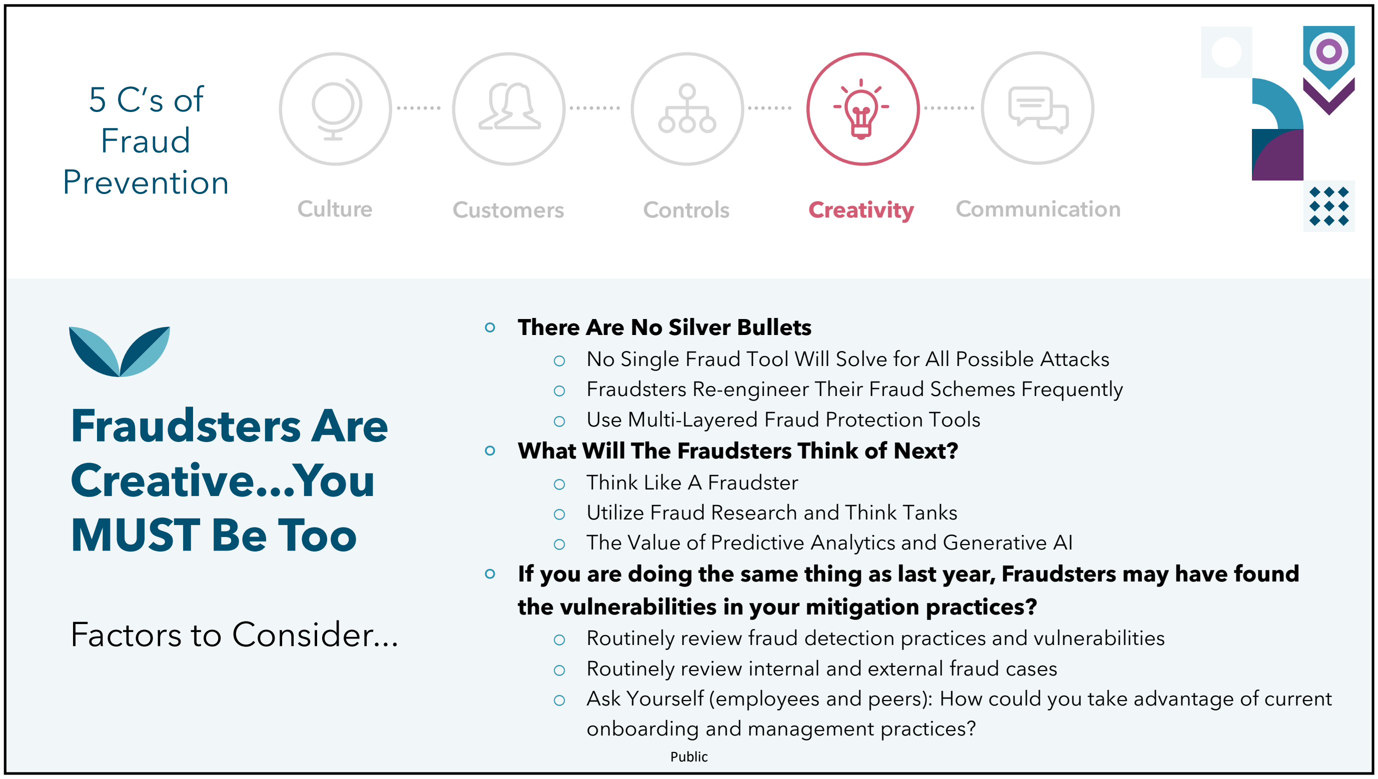
5 C's of Fraud Prevention

Culture · Customers · **Controls** · Creativity · Communication

Define controls before escalation is needed

- **Strong internal controls to help detect, prevent and respond to fraud**
  - Policy
  - Procedures
  - Fraud detection software
- **Segregation of duties and regular audits**

Public



5 C's of Fraud Prevention

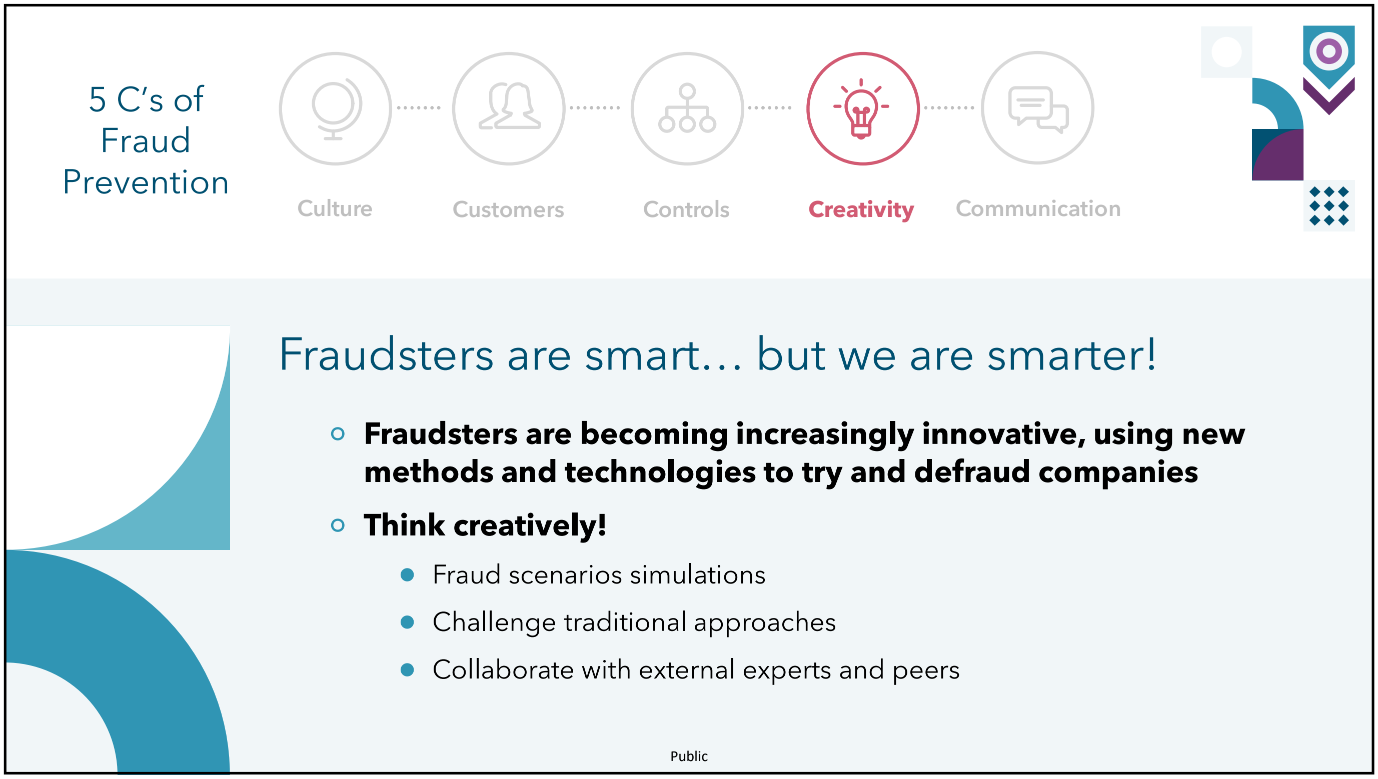
Culture · Customers · Controls · **Creativity** · Communication

Fraudsters Are Creative…You MUST Be Too

Factors to Consider…

- **There Are No Silver Bullets**
  - No Single Fraud Tool Will Solve for All Possible Attacks
  - Fraudsters Re-engineer Their Fraud Schemes Frequently
  - Use Multi-Layered Fraud Protection Tools
- **What Will The Fraudsters Think of Next?**
  - Think Like A Fraudster
  - Utilize Fraud Research and Think Tanks
  - The Value of Predictive Analytics and Generative AI
- **If you are doing the same thing as last year, Fraudsters may have found the vulnerabilities in your mitigation practices?**
  - Routinely review fraud detection practices and vulnerabilities
  - Routinely review internal and external fraud cases
  - Ask Yourself (employees and peers): How could you take advantage of current onboarding and management practices?

Public



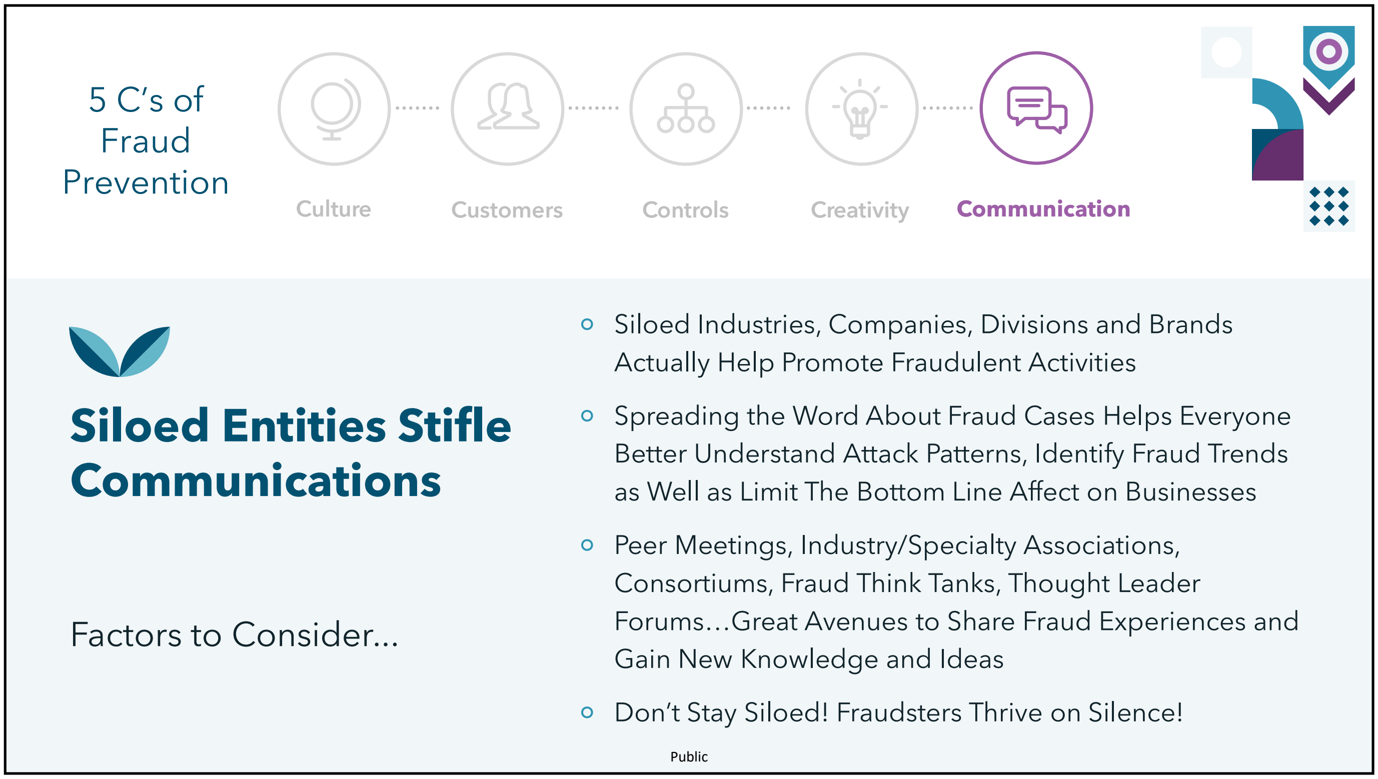
5 C's of Fraud Prevention

Culture · Customers · Controls · **Creativity** · Communication

Fraudsters are smart… but we are smarter!

- **Fraudsters are becoming increasingly innovative, using new methods and technologies to try and defraud companies**
- **Think creatively!**
  - Fraud scenarios simulations
  - Challenge traditional approaches
  - Collaborate with external experts and peers

Public



5 C's of Fraud Prevention

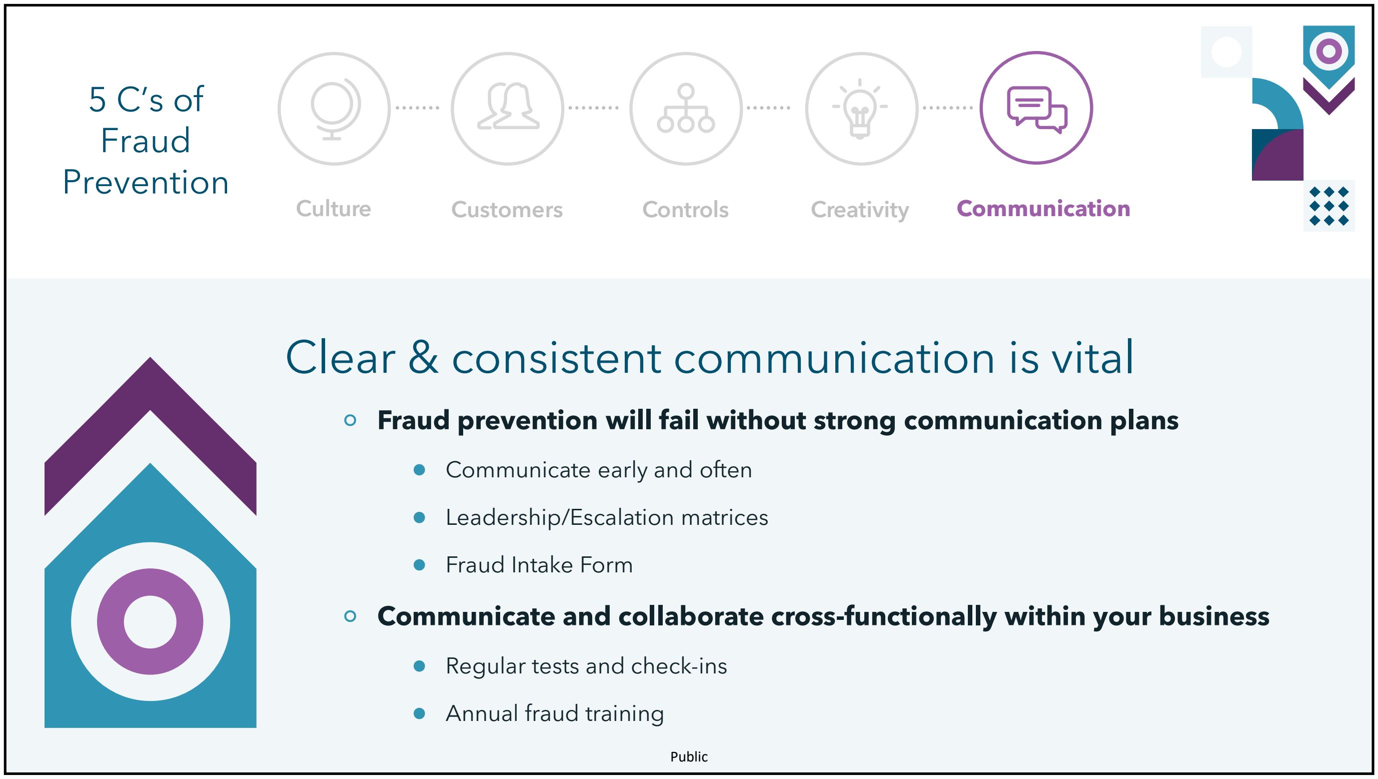
Culture · Customers · Controls · Creativity · **Communication**

Siloed Entities Stifle Communications

Factors to Consider…

- Siloed Industries, Companies, Divisions and Brands Actually Help Promote Fraudulent Activities
- Spreading the Word About Fraud Cases Helps Everyone Better Understand Attack Patterns, Identify Fraud Trends as Well as Limit The Bottom Line Affect on Businesses
- Peer Meetings, Industry/Specialty Associations, Consortiums, Fraud Think Tanks, Thought Leader Forums…Great Avenues to Share Fraud Experiences and Gain New Knowledge and Ideas
- Don't Stay Siloed! Fraudsters Thrive on Silence!

Public



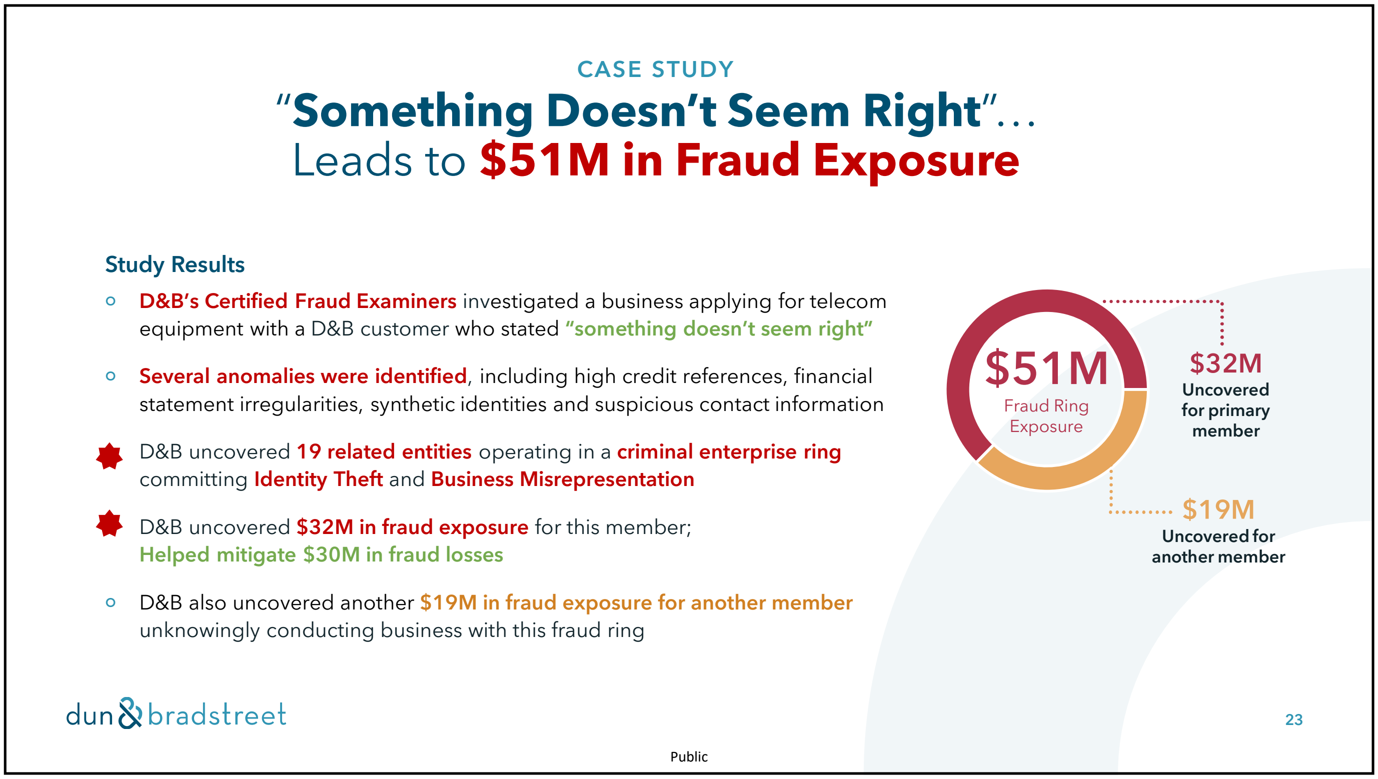
5 C's of Fraud Prevention

Culture · Customers · Controls · Creativity · **Communication**

Clear & consistent communication is vital

- **Fraud prevention will fail without strong communication plans**
  - Communicate early and often
  - Leadership/Escalation matrices
  - Fraud Intake Form
- **Communicate and collaborate cross-functionally within your business**
  - Regular tests and check-ins
  - Annual fraud training

Public



CASE STUDY

"Something Doesn't Seem Right"… Leads to $51M in Fraud Exposure

Study Results

- **D&B's Certified Fraud Examiners** investigated a business applying for telecom equipment with a D&B customer who stated **"something doesn't seem right"**
- **Several anomalies were identified**, including high credit references, financial statement irregularities, synthetic identities and suspicious contact information
- D&B uncovered **19 related entities** operating in a **criminal enterprise ring** committing **Identity Theft** and **Business Misrepresentation**
- D&B uncovered **$32M in fraud exposure** for this member; **Helped mitigate $30M in fraud losses**
- D&B also uncovered another **$19M in fraud exposure for another member** unknowingly conducting business with this fraud ring

$51M Fraud Ring Exposure

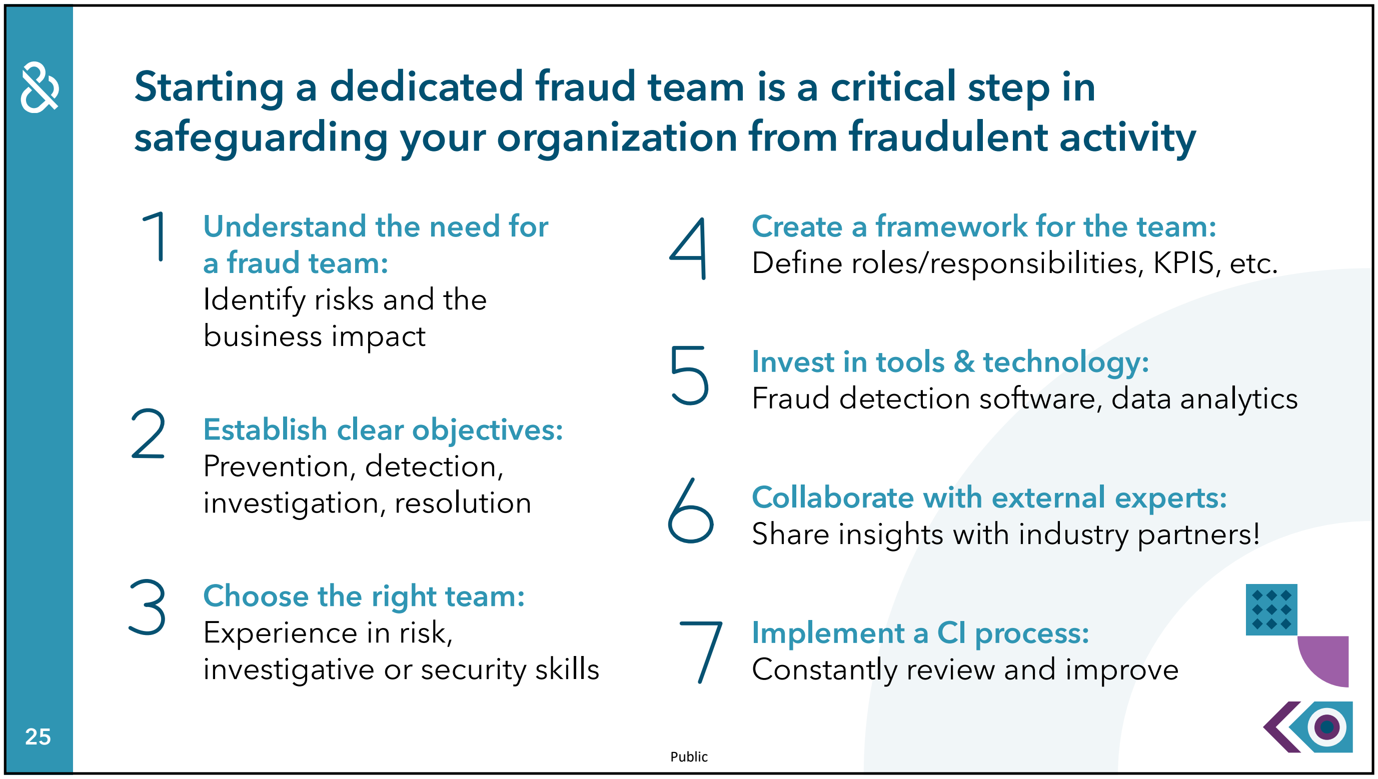
$32M Uncovered for primary member

$19M Uncovered for another member

dun & bradstreet 23

Public

How to Establish a Dedicated Fraud Team



Starting a dedicated fraud team is a critical step in safeguarding your organization from fraudulent activity

1 **Understand the need for a fraud team:** Identify risks and the business impact

2 **Establish clear objectives:** Prevention, detection, investigation, resolution

3 **Choose the right team:** Experience in risk, investigative or security skills

4 **Create a framework for the team:** Define roles/responsibilities, KPIS, etc.

5 **Invest in tools & technology:** Fraud detection software, data analytics

6 **Collaborate with external experts:** Share insights with industry partners!

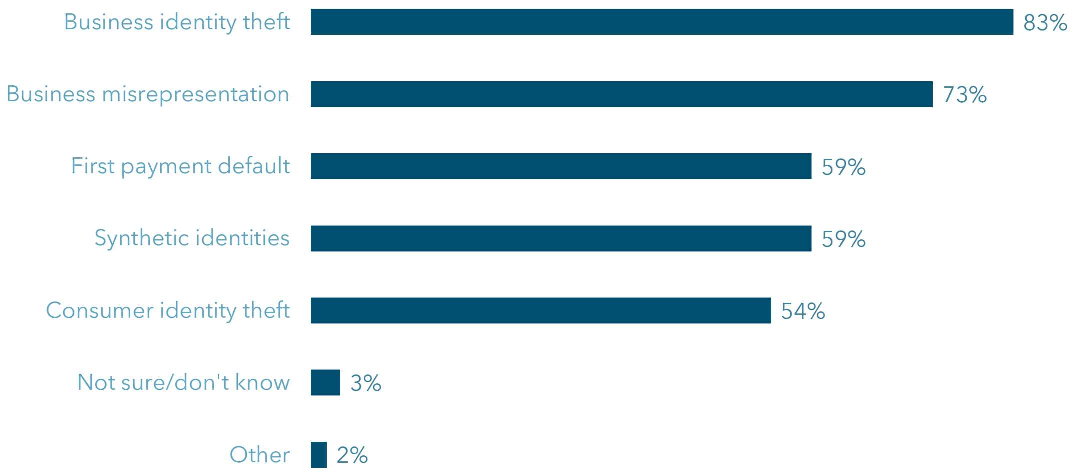
7 **Implement a CI process:** Constantly review and improve

25

Public

A Look at Recent Fraud Trends…

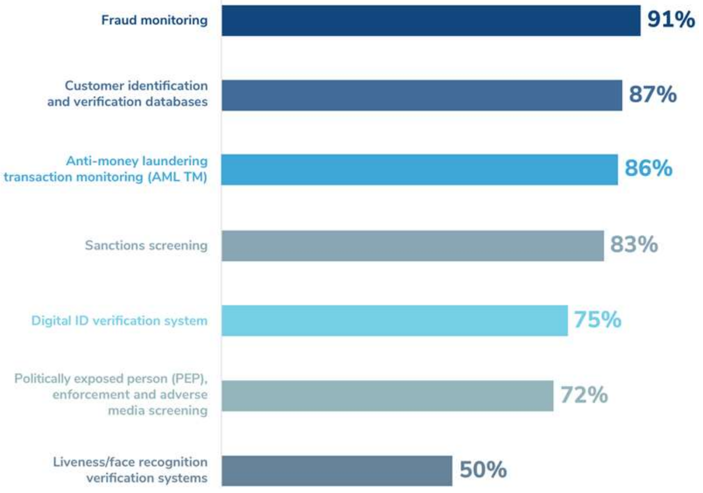
D&B research indicates **Business Identity Theft** as the most prevalent type of Business Fraud



Source: Dun & Bradstreet Fraud Research Studies

Public

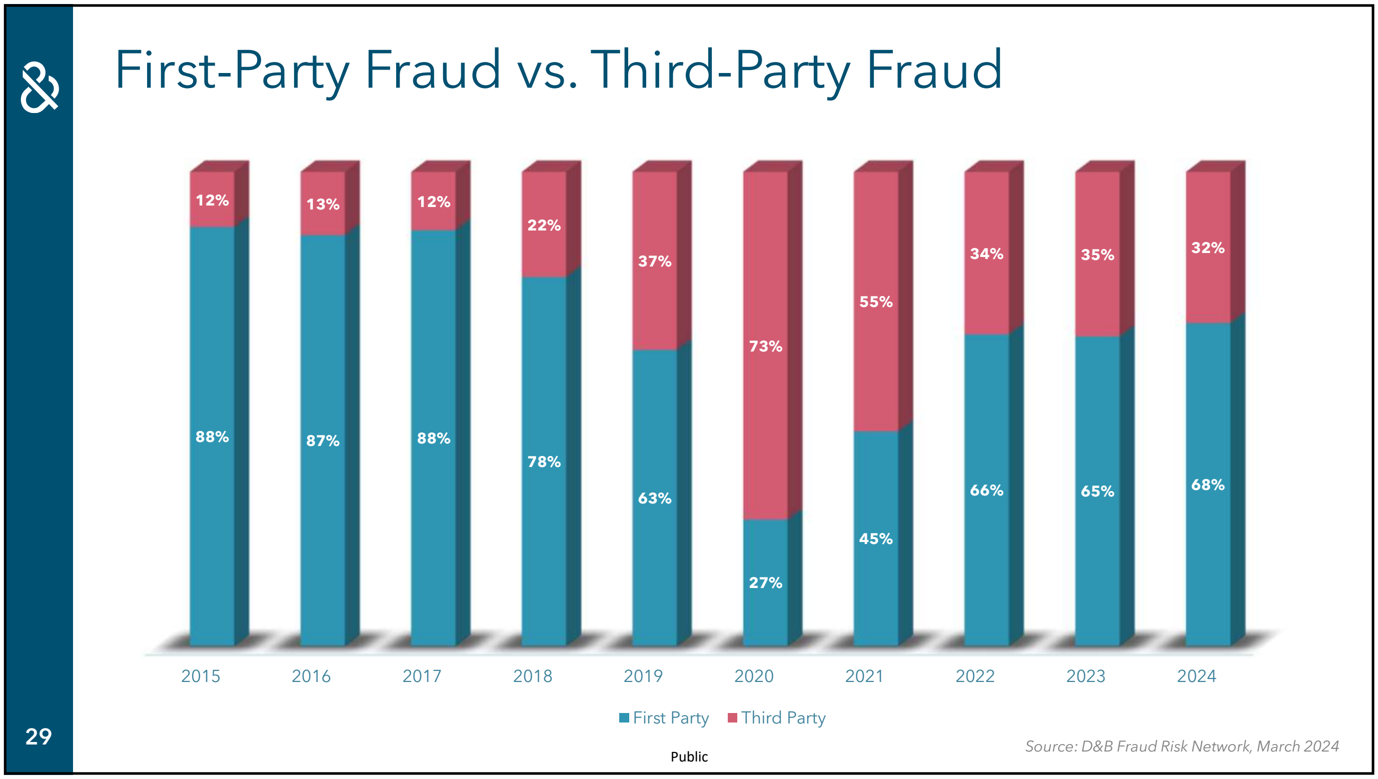
Kroll: Which of the Following Financial Crime Tools are Most Commonly Used?



Source: 2023 Kroll Fraud and Financial Crime Report (p. 15)

28

Public

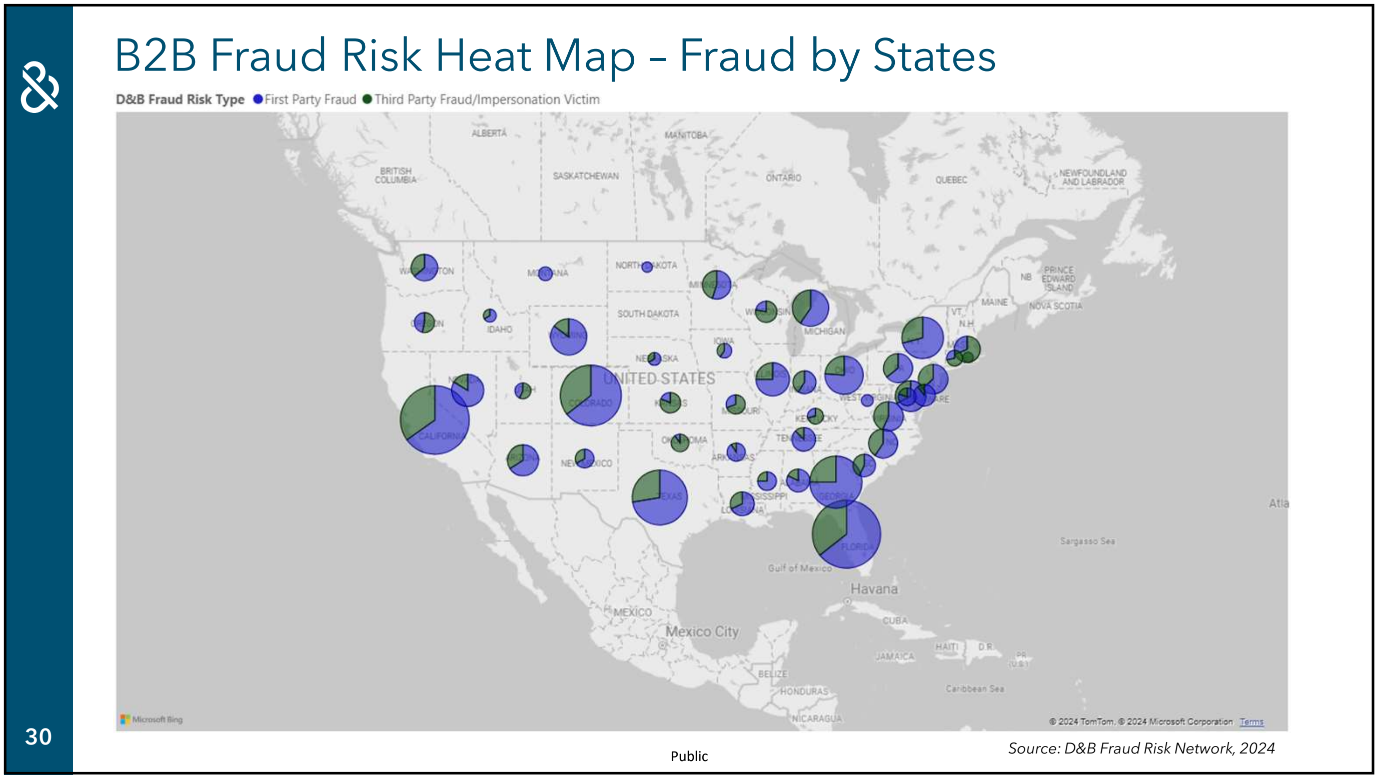


First-Party Fraud vs. Third-Party Fraud

Source: D&B Fraud Risk Network, March 2024

Public

29



B2B Fraud Risk Heat Map – Fraud by States

D&B Fraud Risk Type ● First Party Fraud ● Third Party Fraud/Impersonation Victim

Source: D&B Fraud Risk Network, 2024

Public

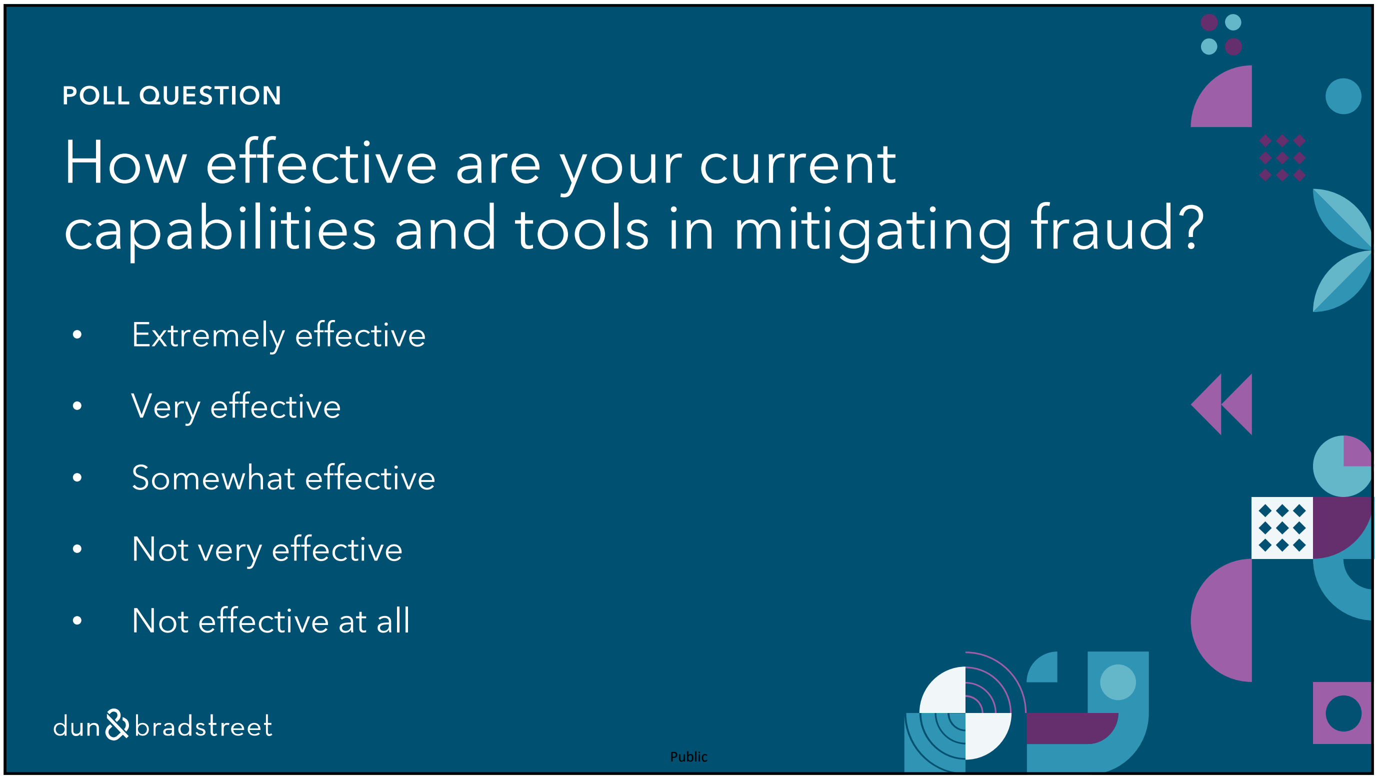
30

B2B Fraud Mitigation Practices

B2B Fraud Mitigation Best Practices

Good Data	Verification	Validation
Data Analytics	Internal Fraud Tools	External Fraud Tools

“Fraud Mitigation Tools Are Only As Good As the Data And Analytics Supporting Them…
Ensure That You Continuously Have Good, Fresh Data and Expert Analytics”



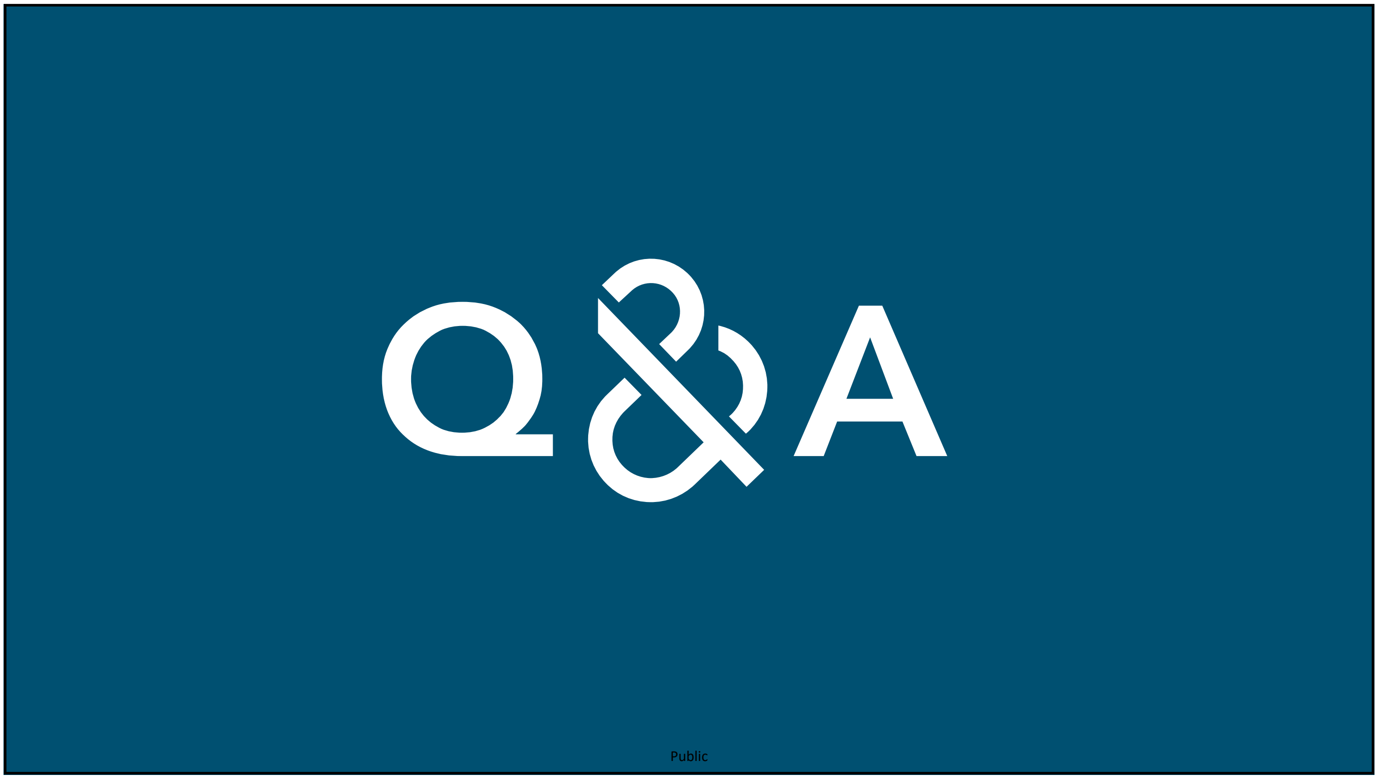
POLL QUESTION

How effective are your current capabilities and tools in mitigating fraud?

- Extremely effective
- Very effective
- Somewhat effective
- Not very effective
- Not effective at all

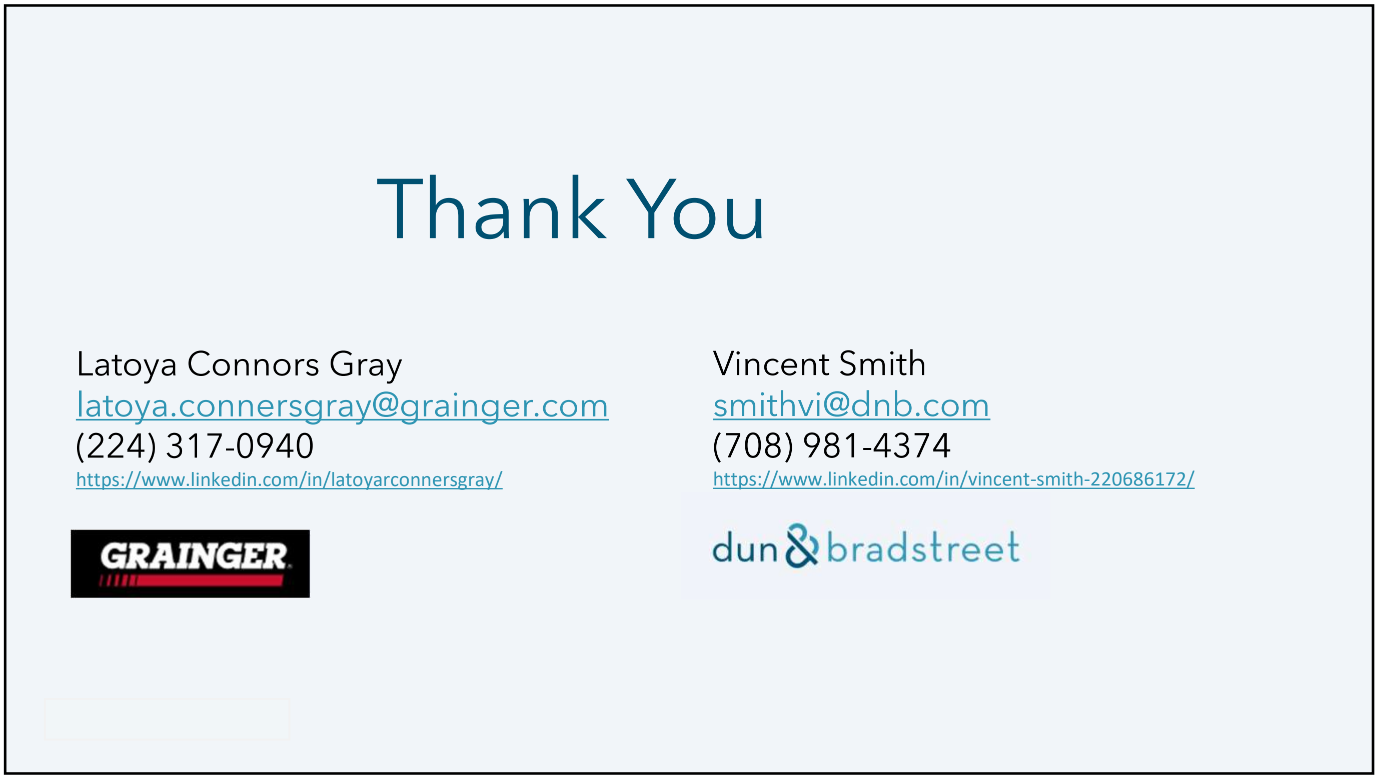
dun & bradstreet

Public



Q&A

Public



Thank You

Latoya Connors Gray
latoya.connersgray@grainger.com
(224) 317-0940
https://www.linkedin.com/in/latoyarconnersgray/

GRAINGER

Vincent Smith
smithvi@dnb.com
(708) 981-4374
https://www.linkedin.com/in/vincent-smith-220686172/

dun & bradstreet