Grant Thornton

Think Like a Fraudster

2020 Fraud Conference

November 23, 2020

Speakers

James Ruotolo
Senior Manager
Fraud Risk Mitigation
T +1 860.781.6744
E james.ruotolo@us.gt.com

Taylor Larimore
Senior Manager
Fraud Risk Mitigation
T +1 215 701 8866
E taylor.larimore@us.gt.com

Agenda

01	**Fraudster 101**	15’
02	**Thinking like a fraudster**	15’
03	**Fraud risk identification**	20’
04	**Solution toolkit**	20’

Grant Thornton

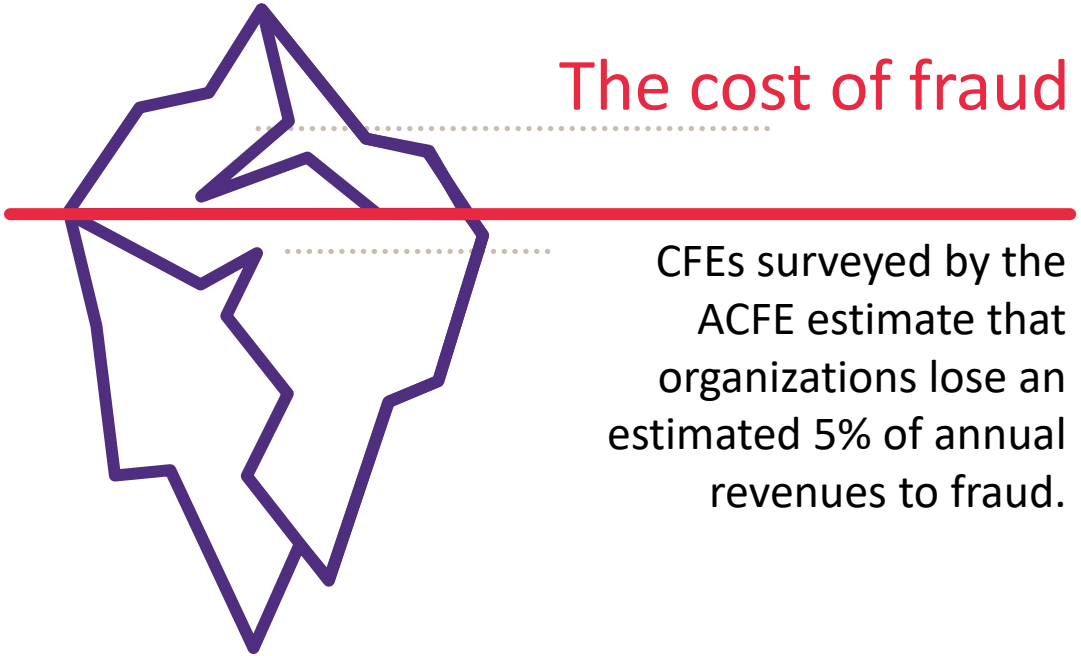
Fraudster 101

Grant Thornton

The cost of fraud

Fraud is like the proverbial iceberg; the deceptive nature of fraud means that it is unknown until discovered, leading to potential ‘submerged’ or unknown frauds beneath the surface.

According to the Association of Certified Fraud Examiners (ACFE), CFEs estimate that organizations around the world lose an estimated 5% of their annual revenues to fraud. Applied the 2019 Gross World Product (GWP), this amounts to **$4.3 trillion** in potential global fraud losses.



Fraudster Profiles

A look at the people who commit fraud and the types of fraud they commit

Well-respected employees are 4x more likely to commit fraud than someone with a poor reputation.

Fraudsters who have been **with their company longer** stole twice as much.

Only 4% of perpetrators had a prior fraud conviction.

Losses caused by men are 72% larger than losses caused by women.

Sources:
KPMG Global profiles of the fraudster
ACFE 2020 Report to the Nations

The Evolution of the Modern Fraudster

Data is the most valuable commodity in modern commercial economies.

SYSTEM HACK

Nefarious actors sell, trade, and weaponize data on a massive scale to gain access to accounts, create fictitious identities, and commit large-scale fraud.

Credential stuffing is a type of brute-force cyber attack where a fraudster tests large numbers of compromised credentials against other log-in applications

Web conferencing hacks are increasing since the COVID-19 outbreak started; registering conference-themed domains later used for malicious purposes

Deep fakes are synthetic media recordings that utilize machine learning technology to create fictitious audio or video

DIY fraud "how-to" guides are available to teach a new generation of cybercriminals to defraud organizations and their customers

Grant Thornton

The Rise of the Dark Web

The dark web offers anonymity to bad actors to conduct illicit business

Data records are lost or stolen at the following frequency

Everyday	Every hour	Every minute	Every second
5,982,772 records	249,2822 records	4,155 records	69 records

Source: breachlevelindex.com

IT'S A BUYER'S MARKET

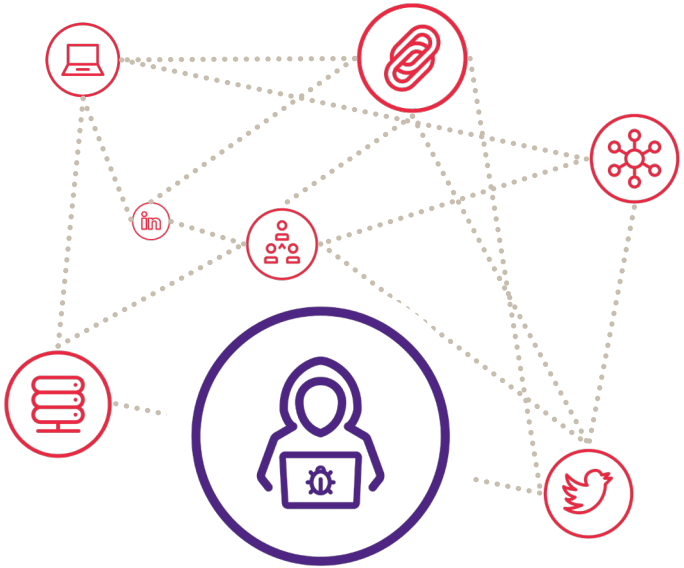
"The Onion Router," (Tor), is the most popular and prolific browser for accessing the dark web.

Marketplace

$0-$100	$200-$350	$500-$1,000	$5,000-$500,000
Credit cards with T2	Bomb threat as a service	Malware	Hits
Freshly hacked emails	Biological material	Access to government networks	Money laundering
DDOS attacks			0-days
Hacked websites			

Grant Thornton

How is this used to commit fraud?



A synthetic identity crime example

1. **Buy**
   Purchase stolen PII on the dark web.
2. **Build**
   Create synthetic identity by combining PII with bogus info.
3. **Apply**
   Apply for credit and rapidly mature a credit profile.
4. **Bust Out**
   Use all available credit and disappear.

Grant Thornton

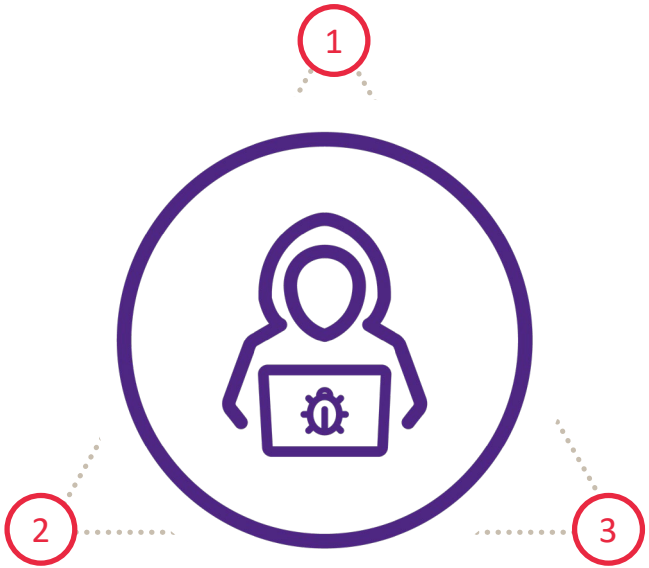
Grant Thornton

Polling Question #1

Thinking like a fraudster

Grant Thornton

Why Do People Commit Fraud?



The Fraud Triangle

1. **Pressure**
   - Bonuses Based on Financial Incentives
   - Investor Expectations
   - Personal Survival
2. **Opportunity**
   - Weak Internal Controls
   - Poor Tone at the Top
   - Inadequate Accounting Policies
3. **Rationalization**
   - “I Deserve It”
   - “I’m only Borrowing a Little”
   - “I’ll Pay it Back”

Thinking Like a Fraudster

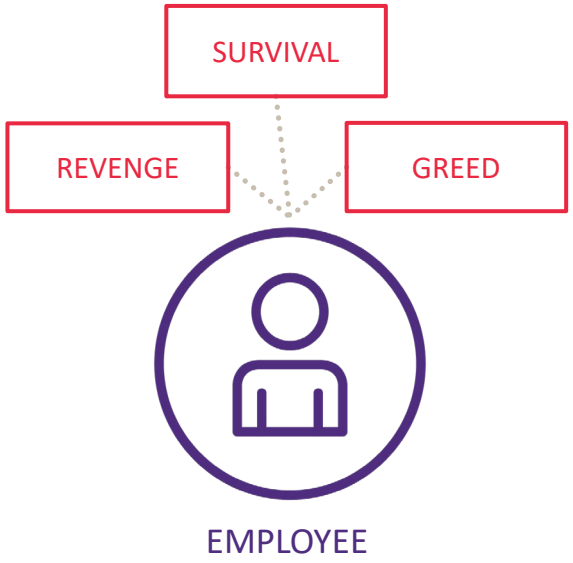
Janet always leaves her computer unlocked. When she steps away, I can steal customer account information from her computer to sell on the dark web.

The company owes me – and it won't hurt anyone if I steal one small check, right?

My supervisor and I both need fast cash – I will add overtime hours to my time sheet and we will split the profits.

Why do good people go bad?

85% of all fraudsters displayed at least one behavioral red flag listed here while committing their crimes



Behavioral Red Flags

42% living beyond means

26% financial difficulties

19% close association with vendor/customer

15% unwillingness to share duties

13% Irritability, suspiciousness, or defensiveness

13% "Wheeler-dealer" attitude

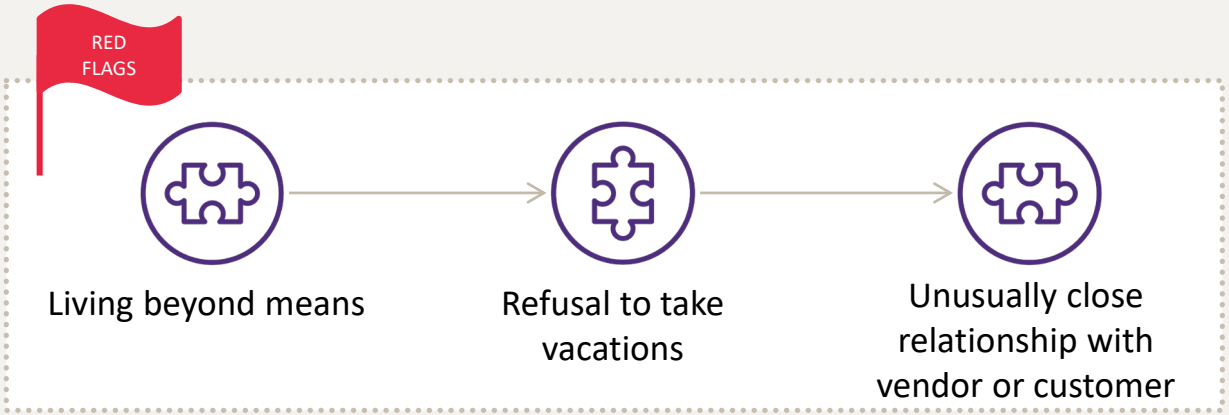
12% divorce/family problems

Employee A

GREED

Frauds perpetrated by individuals motivated by greed are often authoritative figures, those who go unchallenged, or simply remove those who dare to question or interfere.

These individuals think they're better, smarter, more skilled, or superior, thus entitling them to money, titles, authority, perks, and services.



Employee B

SURVIVAL

Corporate survival occurs when employees **falsify information** to increase profits or reduce losses to influence buyers, lenders, or investors to make the company appear to be in a more favorable position.

Personal survival occurs when employees become **financially tapped** because of a personal complication and resort to the only place they have access to … their company.

Employee C

REVENGE

Disgruntled employees may feel improperly compensated or not treated fairly resulting in much higher risk of engaging in criminal behavior. These individuals may feel pressure with an increased workload but little to no reward (e.g., compensation, promotion) driving them to commit fraud and/or harm the company's reputation.

Grant Thornton

Fraud risk identification

Grant Thornton

Fraud Risk Assessment Process

Overview

Identifying Fraud Risks

Understanding the types of fraud that your organization is vulnerable to, both internal and external, is imperative to developing the right antifraud activities.

"Thinking like a fraudster" and coming up with the *fraud schemes that could be used to commit fraud at your organization is a vital step* – ***but where do you start?***

Developing a Fraud Risk Map for your organization is an effective and comprehensive way to identify fraud risks across the enterprise.

What Is a Fraud Risk Map?

A Fraud Risk Map is a resource that identifies potential fraud schemes and other related information for each scheme, such as actor and fraud risk entry point, for various areas within an organization.

Types of Fraud to Consider

Fraud Type	 External Fraud	 Internal Fraud	 Individual Fraud
Definition	Committted by outside organizations, typically by invidiuals or groups, against organizations.	*Aka "Occupational Fraud"* the use of one's occupation for personal enrichment through the deliberate misuse or misapplication of the organization's resources or assets	Devised schemes and actions designed to defraud individuals
Examples	Intellectual Property Theft Insurance Fraud Hacking / Ransomware False Billing Schemes	Corruption Asset Missapropriation Financial Statement Fraud	Identity Theft Ponzi Schemes Phishing Schemes Advanced-Fee Frauds

22

Tips for "Thinking Like a Fraudster"

When identifying fraud schemes, consider the actor (i.e., the perpetrator) and the fraud risk entry points (i.e., the function or process which the actor capitalizes on to carry out the fraud scheme).

When identifying Fraud Schemes, we recommend doing so in a group Conversations with relevant stakeholders will help the group understand the functional area for which frauds schemes are brainstormed.

The Fraud Triangle is a useful model for explaining the factors that cause individuals to commit fraud and can be useful when identifying fraud schemes.

Remember, fraud can be committed either internally (within your organization) or externally (by third parties) and doesn't need to be financial in nature.

Benefits of "Thinking Like a Fraudster"

Thinking like a fraudster will allow you to identify the existing opportunities, motivations, and rationalizations for fraud within your organization.

By extrapolating that information into potential fraud schemes, you can effectively understand the types of fraud that your organization is most vulnerable to, which is imperative to:

1. Understand your existing risks
2. Determine the entry points for fraud at your organization
3. Develop the right antifraud activities for your identified risks

Building Your Fraud Risk Map

At a minimum, your Fraud Risk Map should include information for:

- Related Unit of Analysis (i.e., Department Name or Business Unit)
- Actor
- Fraud Risk Entry Point (or Channel)
- Fraud Scheme

It can include a number of additional elements, such as:

- Fraud Category
- Fraud Type
- Fraud Risk Entry Point Questions
- Internal Vs. External
- Facts & Figures
- Notes/Comments

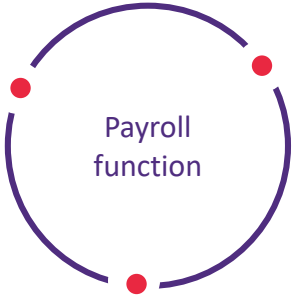
Fraud Risk Map

Fraud risk map example

Fraud creates “leaks” of funding, reducing available funds for legitimate activities

SCHEME
The payroll staff prolongs the pay of an employee who has just left the agency, and alters the payment record so that the direct deposit information is replaced with bank account information of his/her own.
ACTORS

Fraud risk entry point
Payroll records



Fraud risk entry point
Time sheets

SCHEME
Employees pad time sheets, usually in small enough increments to escape the notice of supervisors.
ACTORS

Fraud risk entry point
Payroll system

SCHEME
The payroll staff created a fake employee in the payroll records and falsifies the payment record so that the direct deposit information is replaced with bank account information of his/her own.
ACTORS

The nonfinancial impact of fraud
Fraud encompasses the loss of anything of value, even nonfinancial value – such as PII – which can create other risks, such as reputational compliance, or operational failures and challenges


Payroll staff


Employee

Grant Thornton

Grant Thornton

Polling Question #2

Solution toolkit

Grant Thornton

Solution Toolkit

Organizations should begin by implementing simple cost-effective anti-fraud controls to mitigate their fraud risks.

A lack of internal controls contributes to 1/3 of all frauds perpetrated

Anti-fraud controls

Artificial intelligence	Employee support programs	Surprise audits
Anti-fraud training	Mandatory vacations	Anti-fraud analytics
Anti-fraud policy	Fraud risk assessment	Nudging techniques

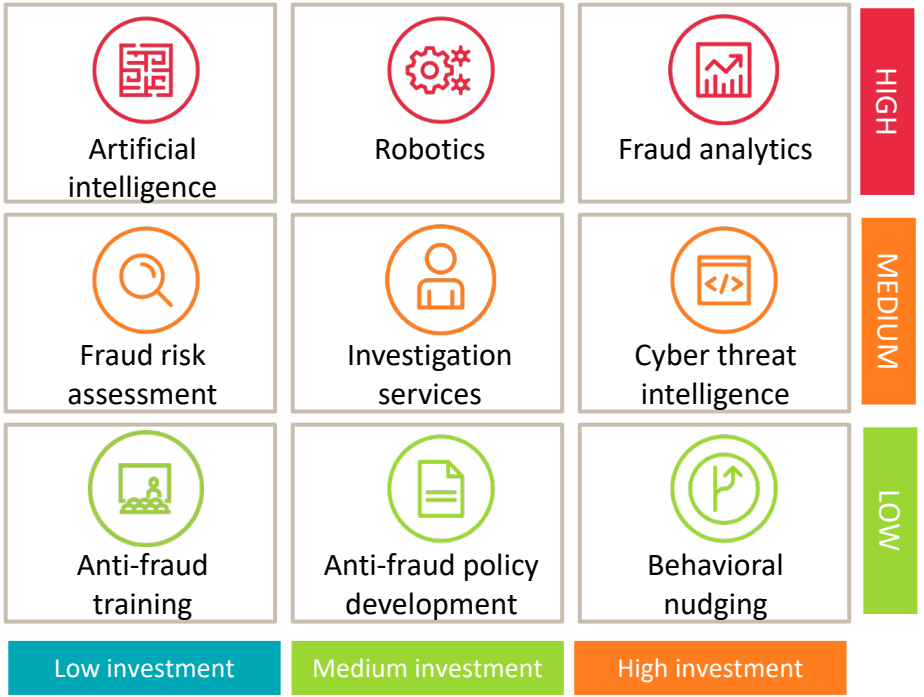
Solution Toolkit

Proactive anti-fraud controls play a key role in an organization's fight against fraud. Organizations should identify a range of solutions and prioritize investments accordingly

Top three control weaknesses

1. Lack of internal controls
2. Lack of management review
3. Override of existing internal controls

Anti-fraud controls matrix

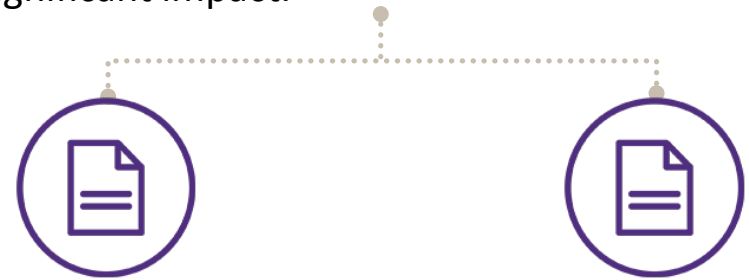


Grant Thornton

Human Behavior

By combining elements of data science and behavioral science, organizations can take action to encourage individuals to be more honest and consistent in their behaviors

- Organizations spend a lot of time and money to combat fraudulent activity; however, they often overlook more common causes of fraud, such as misrepresentations of information (i.e., individuals telling small lies to obtain benefits and/or services to which they are not entitled).
- In the example below, the deployment of a simple behavioral technique, such as including the name of the filer's town, can have a significant impact.



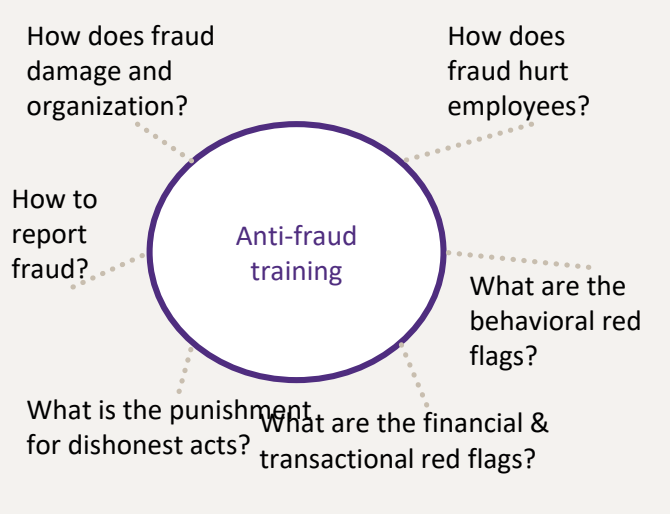
TAX STATEMENT
"Nine out of ten people in your town honestly fill out their tax form."

TAX STATEMENT
"Nine out of ten people in Arlington, VA, honestly fill out their tax form."

Grant Thornton

Fraud Training & Awareness

Organizations should continually deploy anti-fraud training initiatives and develop their fraud awareness programs to harness the full efforts of all employees to significantly reduce the cost of fraud.



Benefits!

- Supports tone at the top
- Alerts employees to red flags
- Reinforcing reporting mechanisms
- Strengthens employee morale
- Strengthens prevention and detection

Grant Thornton

Fraud Risk Assessment

Organizations conduct fraud risk assessments to identify and understand the risks to their business and weaknesses in controls that present a fraud risk to the organization.

Once a risk is identified, a plan can be developed to mitigate those risks by instituting controls or procedures and assigning individuals to monitor and effectuate the plan of mitigation. It is important to update these assessments on an ongoing basis.

Benefits!

- Encourages open conversations about risks at all levels
- Facilitates the ranking of risk priorities
- Identifies and escalated the most significant risk issues
- Informs senior management of risk issues
- Allows an organization to see the overall risk profile
- Facilitates the review and monitoring of risk

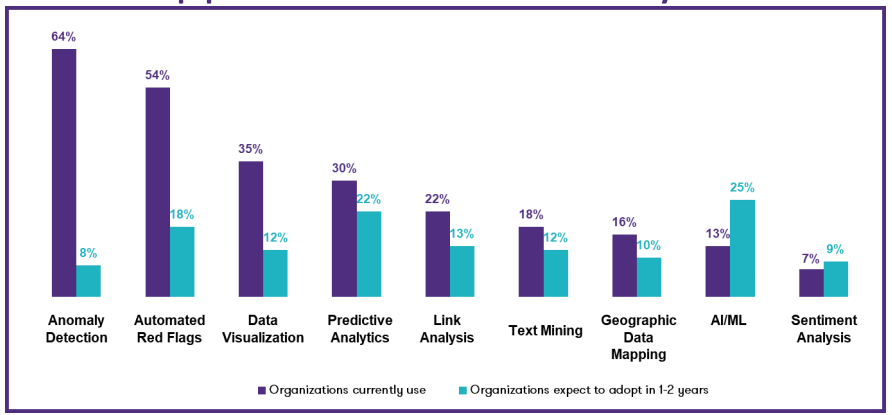
Grant Thornton

Analytics

A variety of techniques and technologies can be used to analyze data to identify red flags and control gaps that might point towards fraudulent behavior.

- To address the challenges and combat the loss of billions of dollars to fraud each year, organizations must establish programs and initiatives geared towards antifraud analytics and detecting fraudulent behavior in real time.
- Organizations are deploying AI/machine learning, risk analytics, behavioral analysis, and biometrics as best practices and innovative techniques to move their focus from a reactive to a preventative approach to fraud.

Approach to Fraud Analytics



Fraud Threat Intelligence

The dark web is just another part of the internet, and the internet is a tool that creates wider access and broader impact for users' goals.

Cybercriminals operate in an underground network, but in the last few years, threat intelligence has evolved with the tools to watch them and act before they can do real damage. Today, most large commercial businesses have widely adopted threat intelligence and digital risk protection programs to inform themselves of how bad actors are targeting them.

Be Prepared

- Do we deploy state of the art of multi-factor authentication to protect against stolen credentials?
- How updated are our firewalls?
- Do our employees, clients, and third-party partners understand the precautions to thwart phishing attempts?
- Are we monitoring the deep and dark web to understand the sophistication and changing dynamics of the modern fraud scheme?
- How vulnerable are we to breached third parties?

Grant Thornton

Questions?

Grant Thornton

Grant Thornton Public Sector helps executives and managers at all levels of government maximize their performance and efficiency in the face of ever tightening budgets and increased demand for services. We give clients creative, cost-effective solutions that enhance their acquisition, financial, human capital, information technology, and performance management. For more information, visit www.gt.com/publicsector.