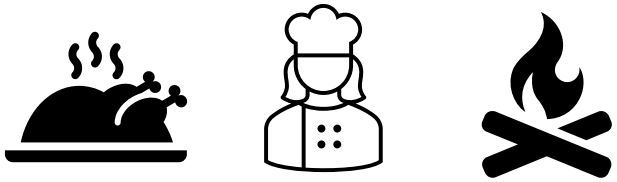
The Frying Pan is Better than the Fire



Mitigating Business Disruption and Fraud Risk during Crises

hfma™
virginia-washington dc chapter

Grant Thornton

Presenter

Bryan Moser
Partner
Forensic Advisory Services
T +1 703 847 7586
E bryan.moser@us.gt.com

Bryan leads the Forensic Advisory Services practice in the DC Metro office. He has nearly 30 years of experience advising clients in risk management and critical business situations, including investigations, compliance and disputes/claims. Bryan serves clients across the healthcare sector, including hospitals, home health providers, physician practices, testing laboratories, universities, services providers and others.

Bryan assists clients with government and internal fraud investigations. Issues include earnings management, billing fraud, embezzlement, FCPA violations, improper vendor arrangements, tax evasion using offshore entities, misappropriation of grant and other government funding and compliance with governmental policies. He assists clients in matters related to compliance with government regulations by analyzing corporate practices and controls. Bryan has performed engagements to monitor financial and operational compliance with contractual and consent agreements and to assess the effectiveness of remediation procedures.

Bryan testifies as an expert witness on complex litigation matters. He assists plaintiffs and defendants in disputes involving breach of contract and other matters, including economic damages and lost profits.

Bryan is a Certified Public Accountant (CPA), Accredited in Business Valuation (ABV) and Certified in Financial Forensics (CFF), and a Certified Fraud Examiner (CFE).

Learning Objectives

1. Describe key elements of a business continuity plan
2. Identify critical business functions susceptible to disruption and fraud
3. Identify fraud risks present when implementing business continuity plans
4. Apply methods for incorporating fraud risk mitigation in business continuity plan
5. Develop strategies for mitigating fraud risk during a crisis

Agenda

1. Business Continuity Planning Framework
2. Fraud risk management
3. Common fraud schemes (quick review from last year)
4. Imbedding fraud risk management in BCP
5. Next Steps to Resilience
6. Q&A

Business Continuity Planning Framework

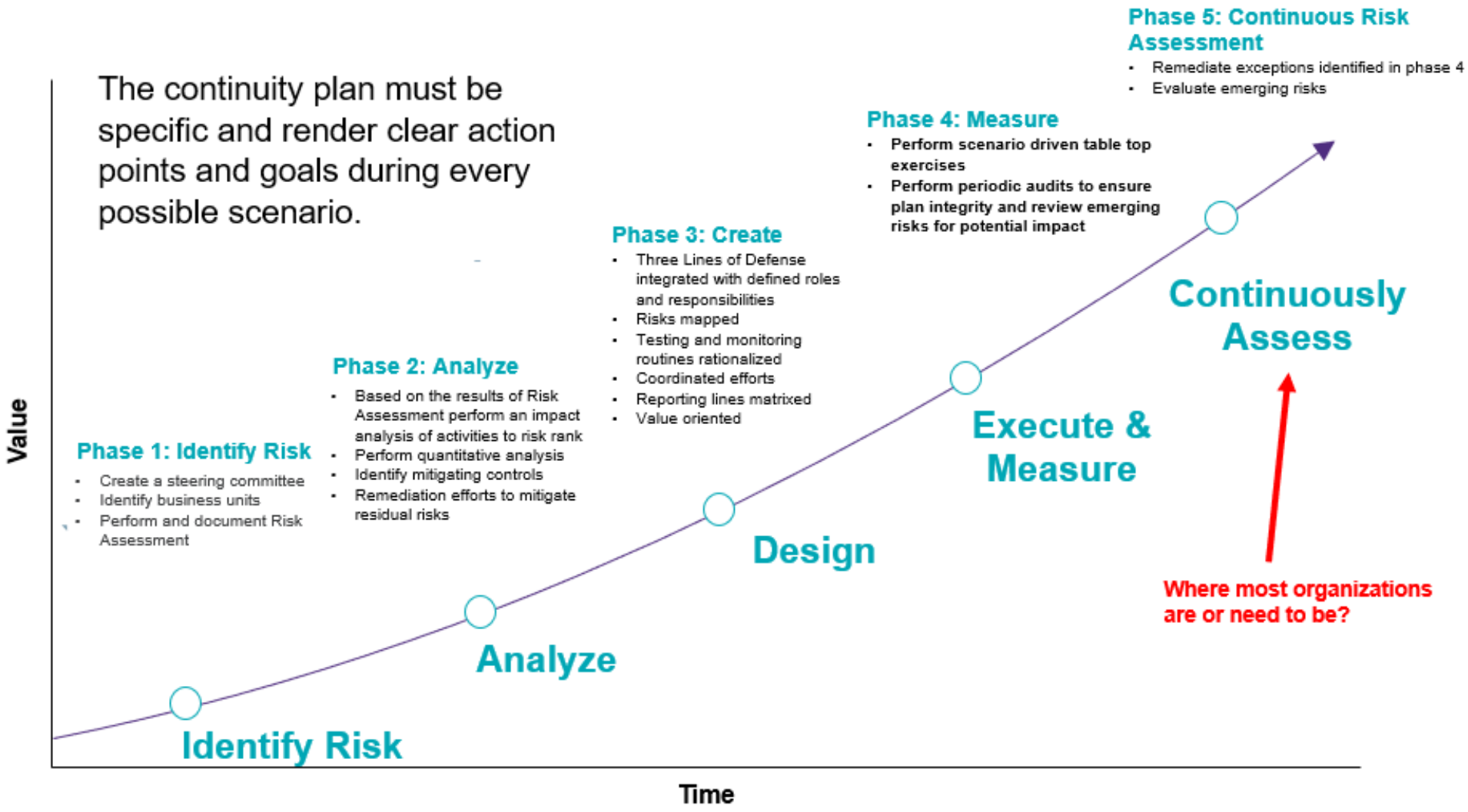
hfma™
virginia-washington dc chapter

Business Continuity Plan Resiliency

BCP goals:

- Serves as a guide for all employees
- Protect all company assets – employees, data, applications, entrusted / custody, etc.
- Response – How is the business operating in a disrupted environment
  - –Impacts to vendors, employees, systems, operations
- Recovery
  - –Changes to the BCP as we identify impacts and look to mitigate risks

BCP – Life Cycle



BCP Risk Assessment

Identify Enterprise Risks

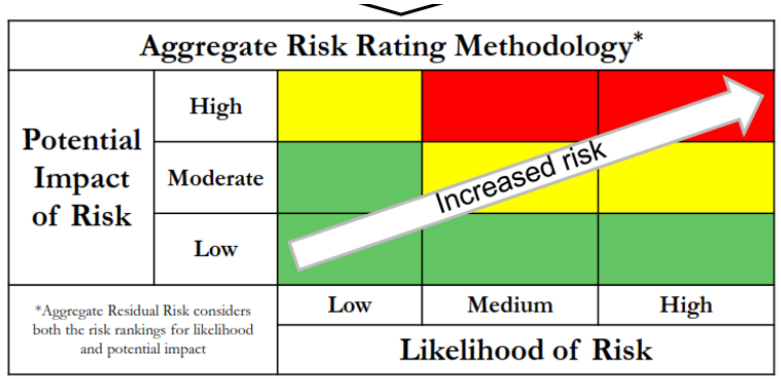
- ✓ Create a steering committee to ensure the focus on all aspects of the entity
- ✓ Perform the risk assessment to identify key risks that could trigger the BCP
  - ✓Facility Risks: fire, flood, other weather
  - ✓Employee Risks: union strike, illness, workplace hazards, government actions
  - ✓Cyber Risks: malware, data breach, network failure, application software failure
  - ✓Fraud risks: intersect with other risks
- ✓ Formally document the risk assessment to help drive the Business Impact Analysis and Business Continuity Plan
- ✓ Ongoing Risk Assessment to include emerging risks

Likelihood of Risk

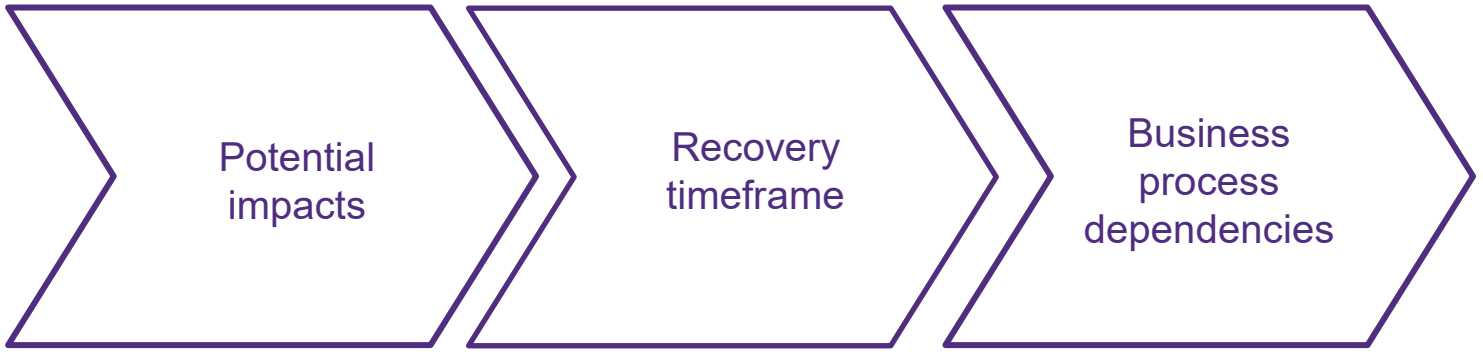
Level	Risk Evaluation Criteria
Low	• Event is unlikely to occur or is not likely to occur
Moderate	• Event may occur in time
High	• Event is more likely to occur

Potential Impact of Risk

Level	Risk Evaluation Criteria
Low	• Minor impact • Require Junior Management and staff attention
Moderate	• Moderate impact • Require Senior/Middle Management attention
High	• Major impact • Require Board/Senior Management attention



Conduct Business Impact Analysis – Quantitative Analysis



- Non-specific events
- Ranking (Low-High)
- Define rankings for consistency

- Recovery point objective
- Recovery time objective
- Maximum allowable downtime

- Third party vendors
- IT systems
- Other business processes

Fraud Risk Management

hfma™
virginia-washington dc chapter

Effective fraud risk management is always important

1. Fraud risk assessment
2. Prevention and detection measures
3. Response readiness

Common fraud schemes
(Review from 2022 Fall Conference)

hfma™
virginia-washington dc chapter

Schemes Common to Healthcare

"Traditional" healthcare industry fraud

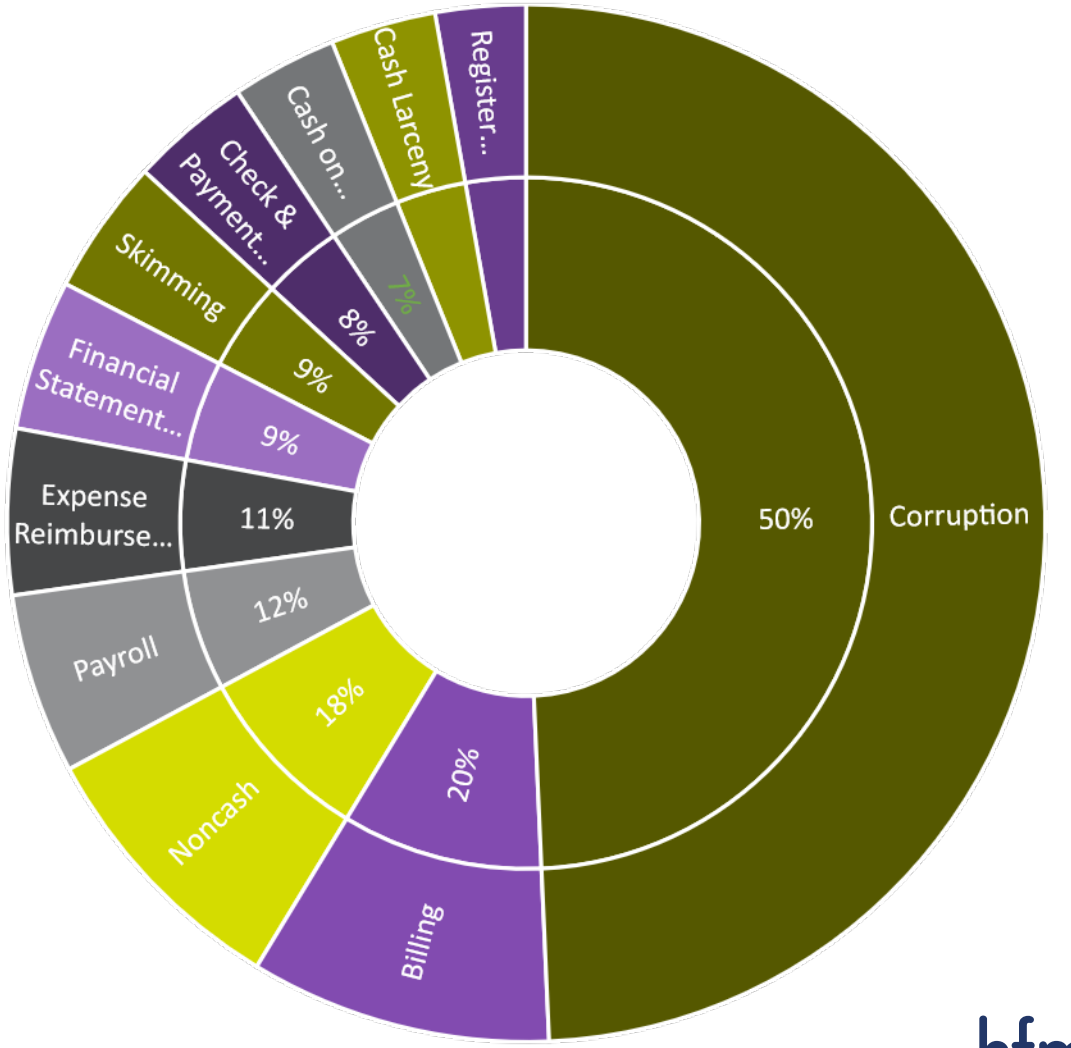
Other non-industry specific

Think outside the billing and coding black box!

Most Common Occupational Fraud Schemes – Healthcare

Top 5:

- Corruption
- Billing
- Non-Cash Asset Schemes
- Payroll Schemes
- Expense Reimbursement



“Traditional” healthcare industry fraud

1. Billing Fraud
   - Billing services not rendered
   - Billing non-covered service as covered
   - Misrepresenting date, location, service, provider, identify
   - Waiving of deductibles and/or co-payments
   - Incorrect reporting of diagnoses or procedures (including upcoding & unbundling)
   - Duplicate claims
   - Overutilization or unnecessary services / drugs
2. Corruption / bribery (kickbacks for referrals)
3. Employee theft of patient identify

Stark / AKS

Referrals
Contracts
- Real estate
- Consulting arrangements
- Free services / training

Fair Market Value

Be proactive:
- Understand business relationship of the transaction / relationship
- Consult legal resources
- Understand fair market value of underlying transaction elements

Other non-industry specific fraud types

Procurement fraud

Construction fraud

Cyber fraud

Financial statement fraud

Expense reimbursement

Non-Cash (theft or misuse, from external sources or employees)

Payroll

Cyber Fraud – Motivations

What are the bad actors after?

- Customer PII
- PHI
- Investment Strategies, Mergers & Acquisitions
- Company and Trade Secrets / IP
- Market Influencer data (insider information)
- Embarrassing personal information (extortion leverage)
- Increasingly…**Digital Assets**

Generally, things you need to generate revenue and run your organization

Cyber Fraud – Challenges

What makes cyber defense so challenging today?

- Increased attack surfaces (pandemic / WFH regimes)
- Poor security hygiene (passwords, MFA, admin privileges)
- Lack of detailed IT asset and data inventories
- Poor data segmentation and data retention practices
- Lack of Incident Response protocols (and practice!)
- Vis-à-vis digital assets, improper security design & monitoring

Imbedding fraud risk management in BCP

hfma™
virginia-washington dc chapter

Imbed fraud risk management in BCP

1. Consider fraud risk in every BCP element
2. Apply lessons learned from the past
   - Incidents experienced
   - Previously identified risks
   - Industry / competitor experience
3. Identify most critical business functions
4. Focus on BCP development . . . prepare for implementation
5. Balance expediency and risk management

Disruption increases fraud risk

Processes

1. Payment processing
2. Accounts receivable
3. Vendors
4. Communications and IT

Environment

1. Accounting and finance resource drain
2. Alternate facilities
3. Government programs

Emerging issues and Challenges

Emerging Issues Affecting Continuity Planning

- Cyber Breaches
- Connectivity of our infrastructures may create more vulnerability
- Communicating with the workforce
- Severe Weather / Pandemics

Unprecedented Challenges for Survival

- Pandemic and infectious disease
- Weather-related events and natural disasters
- War and political risks
- Regulatory and compliance
- Cybersecurity threats

BYOD and Work from Home Opportunities and Risk

Opportunities

- Lower expense if employee buys devices
- Employee responsible for physical damage
- Provides alternative workspace
- Collaboration team software
- Cloud-based Office software and data back-up processes
- Virtual desktop initiatives

Risk

Can’t control how staff uses devices, monitor activity, or ensure hygiene

Higher security risk for corporate data/privacy

Risk of local virus/malware gaining access to network

Enterprise still liable - Insurance coverage?

Work from Home Tips

1. Read emails, new policies and procedures related to disruptions
2. Use internet firewall/VPN
3. Do not improvise and compromise security
4. Expect disruption themed phishing emails
5. Keep lines of communication open, remain connected with colleagues

Next Steps to Resilience

hfma™
virginia-washington dc chapter

Next Steps in Building Resilient Operations

Culture

- Constant communication amongst leadership to all employees and communication at the business unit level.
- Promote a culture that protects all stakeholders

Collaboration

- Work from home wellness programs:
  - Childcare
  - Healthcare

Technology Enablers

- Digital platforms
- Secure cloud computing
- Video conferences (Teams, Zoom, etc…)

Data Analytics

- Trending analysis
- Opportunities to identify top and low performing books of business
- Focus on elevated areas of priority and risk

Global Model

- Reduce risk by creating offshore service model

Key Areas for Business Continuity Planning

- Disruptions to operations
- Disruptions to supply chain
- Financial impacts to cash flow
- Customer-service relations
- Workforce communications
- Information technology
- Coordination efforts across multiple locations

Fraud Risk Cuts across All of these Areas!

Practice tips

- Assess fraud risks now – before the heat is on!
- Remind stakeholders about fraud during crises
    - Prepare communications template now
- Document and revisit
    - Be intentional when making compromises that could increase risk
    - Never to late to reconsider rushed decisions

BCP Considerations

Business resumption:	Focuses on recreating the necessary business process to continue operations. Alternate facilities, equipment, materials safety stock, communications network.
Continuity of leadership:	Establishes senior leadership and command post after a disaster. Outlines roles and authorities, orders of succession.
IT contingency plan:	Details for systems, networks and major application/data recovery procedures.
Crisis communication:	Includes internal and external communication structure and roles. Identifies specific individuals who will communicate with external entities (government, media, staff).
Cyber incident response:	Focuses on damage assessment, securing data, restoring security.
Disaster recovery plan:	Focuses on how to recover various operational and IT mechanisms after a disaster.
Occupant emergency:	Establishes personnel safety and evacuation procedures/alternate workspace.

Incident response

Whistleblower / other allegations

- Document a protocol
- Assign a team

Investigation approach

- See above
- Know who to call

Remediation

- AVOID temptation to cut corners

Fraud after the disruption

Reassess risks of altered working environment

Questions to ask

- How have things changed?
- Are things really back to normal (ever)?
- Have new risks appeared?
- Did you change access, approvals and processes during the disruption?

Anti-Fraud measures

1. Principled Tone at the Top
2. Monitor and Follow Up on Employee Hotline
3. Document and Reinforce Code of Conduct
4. Hiring and Promoting Appropriate Employees
5. Continuous Training and Communications
6. Administer Fair and Balanced Discipline
7. Acquisition due diligence
8. Engage Independent External Legal / Consultant if Fraud Is Suspected

Any final questions?

hfma™
virginia-washington dc chapter

hfma

virginia-washington dc chapter

Bryan Moser
Partner, Grant Thornton LLP
Forensic Advisory Services
T 703 847 7586
E Bryan.Moser@us.gt.com

vadchfma.org

Disclaimer

This Grant Thornton LLP presentation is not a comprehensive analysis of the subject matters covered and may include proposed guidance that is subject to change before it is issued in final form. All relevant facts and circumstances, including the pertinent authoritative literature, need to be considered to arrive at conclusions that comply with matters addressed in this presentation. The views and interpretations expressed in the presentation are those of the presenters and the presentation is not intended to provide accounting or other advice or guidance with respect to the matters covered

For additional information on matters covered in this presentation, contact your Grant Thornton LLP adviser

Disclaimer

* *

IRS Circular 230 disclosure: To ensure compliance with requirements imposed by the U.S. Internal Revenue Service, we inform you that any U.S. federal tax advice contained in this PowerPoint is not intended or written to be used, and cannot be used, for the purpose of (a) avoiding penalties under the U.S. Internal Revenue Code or (b) promoting, marketing or recommending to another party any transaction or matter addressed herein.

* *

The foregoing slides and any materials accompanying them are educational materials prepared by Grant Thornton LLP and are not intended as advice directed at any particular party or to a client-specific fact pattern. The information contained in this presentation provides background information about certain legal and accounting issues and should not be regarded as rendering legal or accounting advice to any person or entity. As such, the information is not privileged and does not create an attorney-client relationship or accountant-client relationship with you. You should not act, or refrain from acting, based upon any information so provided. In addition, the information contained in this presentation is not specific to any particular case or situation and may not reflect the most current legal developments, verdicts or settlements.

You may contact us or an independent tax advisor to discuss the potential application of these issues to your particular situation. In the event that you have questions about and want to seek legal or professional advice concerning your particular situation in light of the matters discussed in the presentation, please contact us so that we can discuss the necessary steps to form a professional-client relationship if that is warranted. Nothing herein shall be construed as imposing a limitation on any person from disclosing the tax treatment or tax structure of any matter addressed herein.

© 2021 Grant Thornton LLP, the U.S. member firm of Grant Thornton International Ltd. All rights reserved. Printed in the U.S. This material is the work of Grant Thornton LLP, the U.S. member firm of Grant Thornton International Ltd.