NAVIGATING THE CYBERSECURITY LANDSCAPE: SEC REGULATION AND ENFORCEMENT

Association of Corporate Counsel Chicago Chapter

James Vinocur | Stephen Reynolds | Caitlyn Campbell | Paul Helms

December 2024

mwe.com

ACC Association of Corporate Counsel CHICAGO

McDermott Will & Emery

INTRODUCTION

James Vinocur | Senior Corporate Counsel, Baxter

Experience with Cybersecurity, AI, and White Collar Matters

Member, Cyber Counsel Group

Former Prosecutor, Manhattan District Attorney's Office

Stephen Reynolds | Partner, Chicago Office

Former Computer Programmer and IT Analyst

Advises on Complex Data Security and Privacy Matters

CIPP/US, CISSP

INTRODUCTION

Caitlyn Campbell | Partner, Boston Office

Former Senior Counsel to SEC Directors of Enforcement in DC and Enforcement Attorney in Boston

Liaison to Financial Reporting and Audit Group

Paul Helms | Partner, Chicago Office

Former Counsel to SEC Director of Enforcement in DC and SEC Enforcement Attorney in Chicago

Asset Management Unit and CAIA Credential

TOPICS

- Anticipated effect of the election on SEC cybersecurity enforcement efforts
- Guidance from the SEC on the cybersecurity rules that went into effect in December 2023
- Recent SEC cybersecurity enforcement actions
- Practical strategies in-house counsel can employ to manage risk

ELECTION UPDATE

ELECTION UPDATE | CURRENT COMMISSION

Gary Gensler

Hester Peirce

Caroline Crenshaw

Mark Uyeda

Jaime Lizárraga

ELECTION UPDATE | NEW CHAIR

Paul Atkins

- SEC Commissioner from August 2002 to August 2008
- Appointed by President George W. Bush
- Served on the staff of two former Chairs, Richard Breeden and Arthur Levitt, from 1990 to 1994

ELECTION UPDATE | CURRENT DIVISION LEADERS

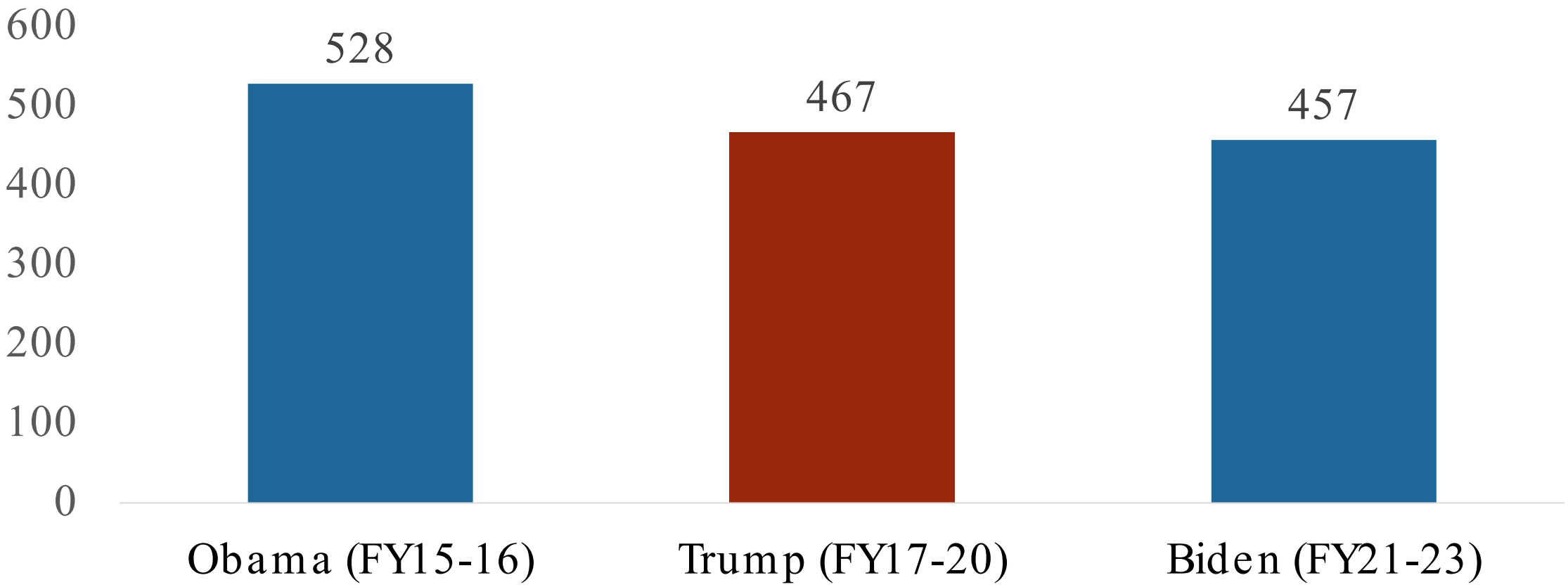
Sanjay Wadhwa
Acting Director

Sam Waldon
Acting Deputy Director

ELECTION UPDATE | EXPECTATIONS

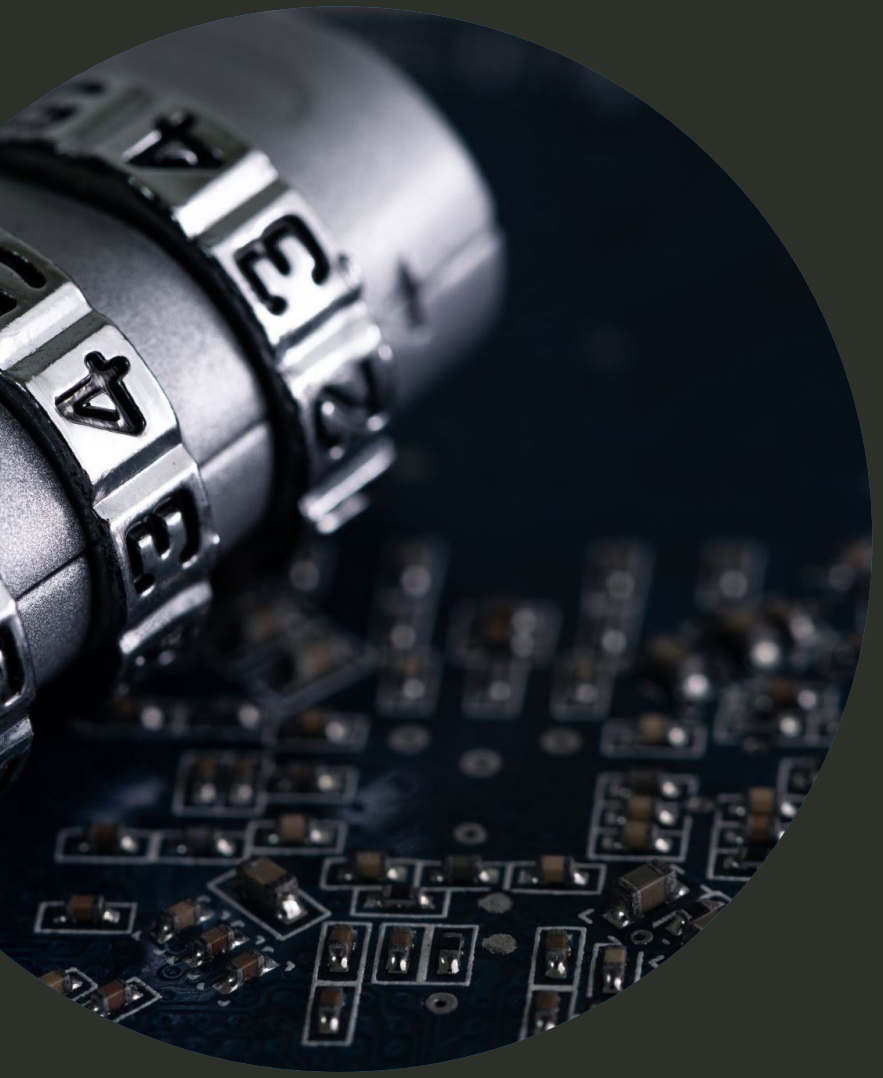
- SEC enforcement efforts tend to be relatively bipartisan
- Examination and enforcement staff remains relatively constant, and long-tailed investigations take time to work through the system
- Staff will work to enforce existing regulations, such as the newly-minted cybersecurity disclosure requirements
  - For example, cybersecurity is a bipartisan national security interest, particularly in the context of the financial markets
  - Chair Clayton pursued regulatory and enforcement agenda, although more careful not to punish victimized public companies
- Changes are likely to come in the form of emphasis, with more resources devoted to retail-level fraud

ELECTION UPDATE | STAND-ALONE ACTIONS



ELECTION UPDATE | COMING YEAR

- More resource challenges
- Lower penalties
- Continued emphasis on individuals
- More technical and data-driven cases: watch for insider trading
- Potential for recent rule changes to spur additional enforcement



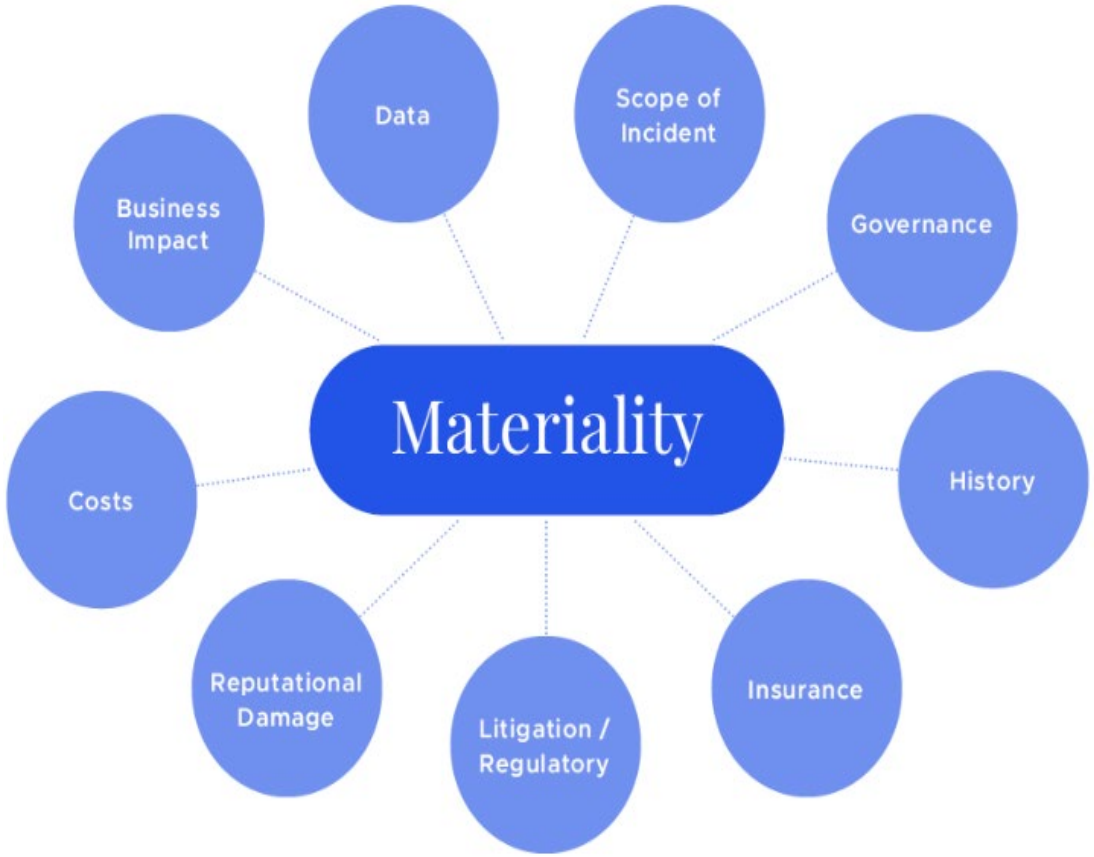
CYBERSECURITY RULES

CYBERSECURITY RULES | INCIDENT DISCLOSURE

- Public companies must file a Form 8-Kwithin four business days of a determination that a cybersecurity incident it has experienced is material
- Specifically, the new Form 8-K1.05 line item requires disclosure of the:
  - Nature, scope and timing of the incident and
  - Its impact or reasonably likely impact on the company

CYBERSECURITY RULES | MATERIALITY

- Rules do not specify how to determine the materiality of a cybersecurity incident
- Instead, materiality is to be evaluated based on the total mix of information
- Prior administration: Should not be limited to the impact on "financial condition and results of operation" and consider qualitative factors
  - Reputational harm
  - Possible regulatory actions
  - Possible litigation



CYBERSECURITY RULES | FORM 8-K

- Companies must amend a previously filed Item 1.05 Form 8-Kto disclose information that was not determined or was unavailable at the time
- Two safe harbor provisions that potentially mitigate liability concerns associated with the proposed new requirements:
  - Form S-3 eligibility
  - Section 10(b) or Rule 10b-5

CYBERSECURITY RULES | FORM 10-K

- Companies required to disclose information regarding their cybersecurity risk management strategies annually
- Specifically, rules add a new Item 106(b) to Regulation S-K to disclose:
  - Company's processes, if any, for the assessment, identification, and management of material risks from cybersecurity threats and
  - Whether any risks from cybersecurity threats have materially affected or are reasonably likely to materially affect their business strategy, results of operations, or financial condition

CYBERSECURITY RULES | FORM 10-K

- Rules require annual disclosure regarding a company's cybersecurity governance at board and management levels
- New Item 106(c) of Regulation S-K requires disclosure of:
  - Board's oversight of risks from cybersecurity threats and
  - Management's role in assessing and managing material cybersecurity risks
- Although the SEC did not adopt the proposed requirement to disclose board expertise, the final rule requires disclosure of the relevant expertise of those responsible for the company's cybersecurity management

SEC ENFORCEMENT ACTIONS

ENFORCEMENT ACTIONS | SEC FRAMEWORK

- Public companies
- Investment advisers and other regulated entities
- Insider trading and market abuse

ENFORCEMENT ACTIONS | SOLARWINDS

- In late 2019, threat actors gained access to SolarWinds' system and inserted malicious code into a SolarWinds platform
- Threat actors then engaged in a series of cyberattacks targeting SolarWinds' platform and customers, culminating in a large-scale cyberattack known as SUNBURST in December 2020
- In 2023, the SEC filed an action against SolarWinds and its CISO alleging:
  - False and misleading statements in public postings and Form 8-K
  - Internal accounting
  - Disclosure controls

ENFORCEMENT ACTIONS | SOLARWINDS

- In July 2024, the District Court dismissed most of the claims:
  - Internal controls provision is limited to accounting controls
  - Isolated process lapses do not support disclosure control violations
  - Initial disclosures were not materially misleading, finding that they "by any measure bluntly reported brutally bad news for SolarWinds," based on what SolarWinds and its CISO knew when filing
- Securities fraud as to a security statement that described SolarWinds' cybersecurity practices and was published on the SolarWinds website and disseminated to its customers was sufficiently pled

ENFORCEMENT ACTIONS | SOLARWINDS REPRISE

- Notwithstanding this setback, the SEC persisted
- In October 2024, the SEC charged four companies with misleading cyber disclosures, paying civil penalties ranging from $1 to $4 million
  - Two companies disclosed information about the cyberattack, but the SEC concluded that the disclosures omitted certain material information
  - The other two companies allegedly did not update an existing risk factor in response to the cyberattack
- Dissent by Peirce and Uyeda

ENFORCEMENT ACTIONS | PRIOR ADMINISTRATION

Action	Allegations
RR Donnelley	Internal accounting control failures related to interaction with third-party managed security services provider
Blackbaud	Failure to disclose the full impact of a ransomware attack despite technology personnel learning that its earlier public statements about the attack were erroneous
Pearson	Risk factor disclosure describing hypothetical risk was false and minimized event in media statement
Altaba (Yahoo)	Despite theft and access of "crown jewels," Yahoo risk disclosures only disclosed hypothetical risk, and Yahoo did not identify during acquisition process

ENFORCEMENT ACTIONS | SECTION 21A REPORT

- In a Section 21A report issued in October 2018, SEC warned public companies that inadequate cybersecurity fraud prevention may violate the internal accounting control provisions
- Two types of cybersecurity scams that victimized nine public companies, which collectively lost nearly $100 million
  - Perpetrators used fake email accounts to request wire transfers from fake email accounts purportedly held by company executives—emphasizing time-sensitive and secretive nature
  - Fraudsters posed as bona fide foreign vendors demanding payment using compromised vendor email addresses and doctored invoice with accurate purchase order and account balance information

ENFORCEMENT ACTIONS | EXPECTATIONS

- Uncertain environment
- New disclosure rules expected to increase enforcement risk
- National security imperative: expect to see continued cases against public companies, investment advisers, and other regulated entities
- Mechanically, change in crypto enforcement could mean more unit resources devoted to cybersecurity cases
- But new Commission likely to be more receptive to argument that company is victim
- More protection or credit for cooperation in cyber cases

PRACTICAL STRATEGIES

PRACTICAL GUIDANCE | PLANNING

PRACTICAL STRATEGIES

- New rules do not require a "quantifiable trigger" for disclosure
- An incident that results in significant reputation harm to a company may not be readily quantifiable but may need to be reported
- Companies should be cautious about describing cybersecurity risks in hypothetical terms when an incident has occurred
- Companies should consider quantifying aspects of the attack to the extent possible, particularly as to financial impact
  - Focus on the duration and scope of the threat actor's access
  - Consider the relevance of the threat actor's identity to a reasonable investor
  - Evaluate number of affected customers and amount of stolen information

PRACTICAL GUIDANCE | MATERIALITY MATRIX

	Description	Considerations
Financial	Direct quantifiable financial impact of an incident	Financial values derived from financial report and SOX thresholds
Operational	Severe operational impact, such as ransomware or denial-of-service	Recovery time objectives significantly breached for transactional systems Or loss of availability to customer data
Data Breach	Personal data or staff data is accessed and exfiltrated	Reportable breach in terms of data protection acts for respective jurisdictions
Scope	Core systems are repeatedly breached	Multiple factors of repeat incidents where core systems were breached even if no data was exfiltrated within current and previous fiscal period
Regulatory	Regulators from key jurisdictions	This may also include the additional reputational damage is a consequence

PRACTICAL STRATEGIES

- SEC may pursue reporting violations, using data analytics to search for outliers, and insider trading
- Update cybersecurity incident plan to incorporate new Form 8-K disclosures and any need to supplement following initial disclosure
- Consider risk factor disclosures and other sections of SEC filings
- Integrate technical staff with employees in disclosure roles, with clear escalation rules
- SEC website includes helpful resources: www.sec.gov/securities-topics/cybersecurity
  - Commission Statement and Guidance on Public Company Cybersecurity Disclosures (Feb. 2018)

PRACTICAL STRATEGIES | 2018 GUIDANCE

Disclosures	Financial Statements	Policies and Procedures
Risk factors	Expenses managing breach	Disclosure controls and procedures
MD&A	Loss of revenue or assets	CEO and CFO certifications
Description of business	Costs and liabilities associated with warranties, breach of contract, recalls, indemnification, and insurance	Code of ethics and insider trading policies
Legal proceedings	Diminished future cash flows and asset impairment	Regulation FD
Board oversight	Effect of rebates or discounts on revenue	

PRACTICAL STRATEGIES | EARLY RANSOMWARE

From: Candidate, Joe <joe.candidate@gmail.com>
Sent: Monday, September 15, 2015 10:58 AM
To: <hrdirector@yourcompany.com>
Subject: Open Position
Attachments: Resume.pdf

Dear HR Director,

Please see my resume attached.

Thanks,

Joe

PRACTICAL GUIDANCE | CHANGE HEALTHCARE

- "On February 12, criminals used compromised credentials to remotely access a Change Healthcare Citrix portal, an application used to enable remote access to desktops. The portal did not have multi-factor authentication. Once the threat actor gained access, they moved laterally within the systems in more sophisticated ways and exfiltrated data. Ransomware was deployed nine days later."

PRACTICAL GUIDANCE | TIMELINE

Feb 21	Feb 28	Feb 29	March	April
The Attack	The Letter	The Confirmation	The Response	The Sequel
Change Healthcare announces that it is taking its systems offline after discovering a cybersecurity threat	BlackCat/ALPHV claims responsibility for the attack and alleges to hold over 6 TB of data	Change Healthcare confirms that BlackCat/ALPHV represented itself as the group behind the attack	Media reports UHG paid a $22 million ransom HHS investigates The government and UHG launch provider funds to support impacted providers	A second ransomware group, RansomHub, demands payment from Change Healthcare and UHG, for the stolen data

PRACTICAL GUIDANCE | SEC FILING

Item 1.05. Material Cybersecurity Incidents.

On February 21, 2024, UnitedHealth Group (the "Company") identified a suspected nation-state associated cyber security threat actor had gained a
the Compan
patients, to
The Compa
duration or
and notified
to Change H
During the
incident at h
As
As of th
financia
fin
Forward-L
This Curren
provisions o
"project," "s
managemen
uncertainties
statements,
materially, f
Looking Sta
undertake to

Explanatory Note

This Amendment No. 2 (the "Amendment") amends the Current Report on Form 8-K filed by UnitedHealth Group Incorporated (the "Company") with the Securities and Exchange Commission on February 22, 2024 (the "Original Report"), as amended by the Current Report on Form 8-K/A filed on March 8, 2024 ("Amendment No. 1" and together with the Original Report are collectively referred to as the "Filed Reports"). Except as set forth in this Amendment, the information included in the Filed Reports remains unchanged.

Item 1.05. Material Cybersecurity Incidents.

As an update to information concerning the Change Healthcare cyberattack contained in the Filed Reports, the Company issued a press release on April 22, 2024, regarding its ongoing data assessment and support for impacted individuals, support for providers and customers with notifications, and Change Healthcare service restoration progress. A copy of the press release is attached to the Amendment as Exhibit 99.1 and incorporated by reference herein.

Item 9.01. Financial Statements and Exhibits.

Exhibit	Description
99.1	Press Release dated April 22, 2024
104	Cover Page Interactive Data File (formatted as Inline XBRL).

ealth Group Incorporated (the
t").
ccess to certain Change
pany isolated the impacted
ompany promptly notified
of the unprecedented cyberattack
suring patient access to care and
e attack. The Company is
ement is investigating the extent
er systems across the Company
ion of key Change Healthcare
s attached to the Amendment as
materially impact the Company's

Exhibit	Description
99.1	Press Release dated March 7, 2024
104	Cover Page Interactive Data File (formatted as Inline XBRL).

PRACTICAL GUIDANCE | RANSOMWARE

Alph
Meridian

https://tcr.sec.gov/TcrExternalWeb/faces/p

- General trading practices or pricing issu
- Manipulation of a security
- Insider trading
- Material misstatement or omission in a
- Municipal securities transactions or publ
- Specific market event or condition
- Bribery of, or improper payments to, fore
- Initial coin offerings and cryptocurrencie
- Other

Please select the specific category th

Failure to file reports

*** Is this supplemental information to a**

No

*** In your own words, describe the con**

We want to bring to your attention a co
recently adopted cybersecurity incident

It has come to our attention that Meridi
and operational information, has failed
the stipulated four business days, as m

Ransomware gang files SEC complaint over victim's undisclosed breach

By Ionut Ilascu November 15, 2023 09:02 PM 0

The ALPHV/BlackCat ransomware operation has taken extortion to a new level by filing a U.S. Securities and Exchange Commission complaint against one of their alleged victims for not complying with the four-day rule to disclose a cyberattack.

QUESTIONS