King & Spalding

Client Alert

Special Matters and Government Investigations

JANUARY 05, 2024

For more information, contact:

Sumon Dantiki
+1 202 626 5591
sdantiki@kslaw.com

Jacqueline Van De Velde
+1 404 572 2450
jvandevelde@kslaw.com

King & Spalding

Washington, D.C.
1700 Pennsylvania Avenue, NW
Suite 900
Washington, D.C. 20006
Tel. +1 202 737 0500

Atlanta
1180 Peachtree Street, NE
Suite 1600
Atlanta, Georgia 30309
Tel. +1 404 572 4600

FBI and DOJ Offer Guidance on SEC Cybersecurity Incident Disclosure Rules

On December 18, 2023, new cybersecurity rules adopted by the U.S. Securities and Exchange Commission (SEC) became effective. Among other things, those rules require SEC registrants to disclose certain information about cybersecurity incidents within four days after determining that the incident is material.

The new SEC rules stipulate that disclosure of material cybersecurity incidents could be delayed for up to 30 days if the U.S. Attorney General or his designee determines that immediate disclosure would pose a substantial risk to national security or public safety and notifies the SEC of such determination in writing. Under certain circumstances, registrants can also seek subsequent 30- and 60-day delay periods.

On December 6, 2023, the Federal Bureau of Investigation (FBI) issued guidance for companies seeking delays in reporting material cybersecurity incidents. The U.S. Department of Justice (DOJ) issued its own guidance on December 12, 2023. This client alert summarizes that guidance.

THE FBI DELAY REQUEST GUIDANCE

The FBI guidance explains that it is responsible for intake of delay requests on behalf of the DOJ. The FBI then coordinates with U.S. government national security and public safety entities on the delay requests before referring the request to DOJ for assessment. The FBI also coordinates requests for any additional delays in reporting.

In its guidance, the FBI outlined ten items that must be included in a registrant's delay request. Those are:

1. The name of the company;
2. The date that the cyber incident occurred;

3. Details – including date, time, and time zone – related to when the victim company determined that the cyber incident was material such that it would require disclosure on Form 8-K or Form 6-K under the SEC cybersecurity rules.
4. Whether the victim company is already in contact with the FBI or another U.S. government agency regarding this incident, and if so, information about the applicable point of contact;
5. A detailed description of the cyber incident, including the type of incident; known or suspected intrusion vectors and identified vulnerabilities; affected infrastructure or data and description of how they were affected; and operational impact of the company;
6. Confirmed or suspected attribution of cyber actors;
7. Current status of remediation or mitigation efforts;
8. Location where cyber incident occurred;
9. Company points of contact for matter and contact details; and
10. Whether company has previously submitted a delay request and if so, details of last DOJ determination and length of delay granted by DOJ if applicable.

The FBI also noted that a delay request would be denied if the registrant failed to report information about a cyber incident immediately after determining that the incident was material.

THE DOJ DELAY REQUEST GUIDANCE

The DOJ guidance outlined how, once the FBI had compiled the delay request, the DOJ would then assess that request. The DOJ explained that its "primary inquiry" would not be whether the underlying cybersecurity incident poses a substantial risk to public safety and national security, but instead whether public disclosure of that incident would threaten public safety and national security.

The DOJ identified four scenarios under which disclosure of some or all of the information required in Item 1.05 of Form 8-K may pose a substantial risk to national security or public safety and thus merit delayed disclosure. They are:

1. The cybersecurity incident involves a technique for which there is not yet a well-known mitigation, and disclosure may lead to additional incidents;
2. The cybersecurity incident primarily impacts a system operated or maintained by a registrant that contains sensitive U.S. government information and disclosure would increase vulnerability to further exploitation;
3. The registrant is conducting remediation efforts for any critical infrastructure or critical systems[i] and that would be undermined by disclosure, such as by revealing that the registrant is aware of the cybersecurity incident; and
4. The U.S. government becomes aware of a cybersecurity incident and believes that disclosure poses a substantial risk to national security or public safety.

On the fourth category, the DOJ explained that the U.S. government may occasionally seek to obtain a registrant's agreement to delay a disclosure. The DOJ offered three example scenarios in which the U.S. government, rather than a registrant, may be aware of a substantial risk to national security and public safety, including: (a) when disclosure would risk revealing a confidential source, information relating to U.S. national security, or sensitive law enforcement information; (b) when the U.S. government is prepared to execute or is otherwise aware of an operation to disrupt

ongoing illicit cyber activity; and (c) where the U.S. government is aware of or conducting remediation efforts for any critical infrastructure or critical system.

NEXT STEPS

The FBI and DOJ guidance documents makes clear that the Attorney General's decisions to grant a national security or public safety exemption to public disclosure of a cybersecurity incident will be based on whether *public disclosure* of a cybersecurity incident—rather than the effects of the cybersecurity incident itself—poses a substantial risk to public safety or national security. Companies should consider updating their cyber incident preparation and response plans both to adhere to the new SEC rules and to account for the FBI and DOJ guidance. In particular, companies should take clear steps to assess the materiality of a cyber incident and create a system for quickly consulting with law enforcement to request delayed reporting of material incidents where disclosure might create such national security or public safety risks.

[i] *See* U.S. Dep't of Just., Department of Justice Material Cybersecurity Incident Delay Determinations (Dec. 12, 2023), https://www.justice.gov/media/1328226/dl?inline ("This category includes systems operated or maintained for the government as well as systems not specifically operated or maintained for the government that contain information the government would view as sensitive, such as that regarding national defense or research and development performed pursuant to government contracts.").

Special Matters & Government Investigations Partners

Gary Adamson
New York
+1 212 556 2113
gadamson@kslaw.com

Adam Baker
New York
+1 212 556 2376
abaker@kslaw.com

Matthew H. Baughman
Atlanta
+1 404 572 4751
mbaughman@kslaw.com

Amy B. Boring
Atlanta
+1 404 572 2829
aboring@kslaw.com

Christopher C. Burris
Atlanta
+1 404 572 4708
cburris@kslaw.com

Craig Carpenito
New York
+1 212 556 2142
ccarpenito@kslaw.com

Steve Cave
Northern Virginia
+1 703 245 1017
scave@kslaw.com

Michael J. Ciatti
Washington, DC
+1 202 661 7828
mciatti@kslaw.com

Patrick M. Collins
Chicago
+1 312 764 6901
pcollins@kslaw.com

Sumon Dantiki
Washington, DC
+1 202 626 5591
sdantiki@kslaw.com

Ethan P. Davis
San Francisco
+1 415 318 1228
edavis@kslaw.com

Alan R. Dial
Washington, DC
+1 202 661 7977
adial@kslaw.com

Zachary Fardon
Chicago
+1 312 764 6960
zfardon@kslaw.com

Ehren Halse
San Francisco
+1 415 318 1216
ehalse@kslaw.com

Zachary J. Harmon
Washington, DC
+1 202 626 5594
zharmon@kslaw.com

Amy Schuller Hitchcock
Sacramento/San Francisco
+1 916 321 4819
ahitchcock@kslaw.com

John A. Horn
Atlanta
+1 404 572 2816
jhorn@kslaw.com

Andrew C. Hruska
New York
+1 212 556 2278
ahruska@kslaw.com

Mark A. Jensen
Washington, DC
+1 202 626 5526
mjensen@kslaw.com

Dixie L. Johnson
Washington, DC
+1 202 626 8984
djohnson@kslaw.com

William Johnson
New York
+1 212 556 2125
wjohnson@kslaw.com

M. Alexander (Alec) Koch
Washington, DC
+1 202 626 8982
akoch@kslaw.com

Yelena Kotlarsky
New York
+1 212 556 2207
ykotlarsky@kslaw.com

Jade R. Lambert
Chicago
+1 312 764 6902
jlambert@kslaw.com

Jamie Allyson Lang
Los Angeles
+1 213 443 4325
jlang@kslaw.com

Raphael Larson
Washington, DC
+1 202 626 5440
rlarson@kslaw.com

Carmen Lawrence
New York
+1 212 556 2193
clawrence@kslaw.com

Brandt Leibe
Houston
+1 713 751 3235
bleibe@kslaw.com

Aaron W. Lipson
Atlanta
+1 404 572 2447
alipson@kslaw.com

William S. McClintock
Washington, DC
+1 202 626 2922
wmcclintock@kslaw.com

Amelia Medina
Washington, DC
+1 202 626 5587
amedina@kslaw.com

Andrew Michaelson
New York
+212 790 5358
amichaelson@kslaw.com

Patrick Montgomery
Washington, DC
+1 202 626 5444
pmontgomery@kslaw.com

Paul B. Murphy
Atlanta/Washington, DC
+1 404 572 4730
pbmurphy@kslaw.com

Grant W. Nichols
Austin/Washington, DC
+1 512 457 2006
gnichols@kslaw.com

Alicia O'Brien
Washington, DC
+1 202 626 5548
aobrien@kslaw.com

Patrick Otlewski
Chicago
+1 312 764 6908
potlewski@kslaw.com

Michael R. Pauzé
Washington, DC
+1 202 626 3732
mpauze@kslaw.com

Olivia Radin
New York
+1 212 556 2138
oradin@kslaw.com

John C. Richter
Washington, DC
+1 202 626 5617
jrichter@kslaw.com

Rod J. Rosenstein
Washington, DC
+1 202 626 9220
rrosenstein@kslaw.com

Daniel C. Sale
Washington, DC
+1 202 626 2900
dsale@kslaw.com

Greg Scott
Sacramento/San Francisco
+1 916 321 4818
mscott@kslaw.com

Richard Sharpe
Singapore
+65 6303 6079
rsharpe@kslaw.com

Kyle Sheahen
New York
+1 212 556 2234
ksheahen@kslaw.com

Michael Shepard
San Francisco
+1 415 318 1221
mshepard@kslaw.com

Aaron Stephens
London
+44 20 7551 2179
astephens@kslaw.com

Cliff Stricklin
Denver
+1 720 535 2327
cstricklin@kslaw.com

Jean Tamalet
Paris
+33 1 7300 3987
jtamalet@kslaw.com

Courtney D. Trombly
Washington, DC
+1 202 626 2935
ctrombly@kslaw.com

Rick Vacura
Northern Virginia
+1 703 245 1018
rvacura@kslaw.com

Richard Walker
Washington, DC
+1 202 626 2620
rwalker@kslaw.com

David K. Willingham
Los Angeles
+1 213 218 4005
dwillingham@kslaw.com

David Wulfert
Washington, DC
+1 202 626 5570
dwulfert@kslaw.com

Sally Q. Yates
Atlanta/Washington, DC
+1 404 572 2723
syates@kslaw.com