The Fine Line Between Fast and Too Fast: Impacts of Updated Regulatory Guidance on Cyber Incident Reporting in the Financial and Critical Infrastructure Sectors

Guest and Dorsey Panelists

Alison Atkins, Assistant General Counsel and Vice President, Cybersecurity, U.S. Bank National Association
Jennifer Smestad, Vice President, General Counsel and Corporate Secretary, Otter Tail Power Company
Robert Cattanach and Jennifer Coates, Dorsey & Whitney LLP

Program Materials

PowerPoint Presentation

Dorsey eUpdates and Blog Posts

Dorsey Blog: *California AG Announces First CCPA Settlement and There is More Enforcement to Come*, Deb Howitt & Austin Chambers (10/3/22)
Available at: https://www.thetmca.com/california-ag-announces-first-ccpa-settlement-and-there-is-more-enforcement-to-come/

Dorsey eUpdate: *Cybersecurity, False Statements and Omissions*, Thomas Gorman (4/27/22)
Available at: https://www.dorsey.com/newsresources/publications/client-alerts/2022/04/cybersecurity-false-statements-and-omission

Dorsey eUpdate: *Utah's New Privacy Law: Will This New Balance Become the Norm?*, Robert Cattanach & Gloria Park (3/21/22)
Available at: https://www.dorsey.com/newsresources/publications/client-alerts/2022/03/utah-new-privacy-law

Session materials are available for download on www.dorsey.com.
Search: "Corporate Counsel Symposium 2022"

CCS | corporate counsel symposium

DORSEY always ahead

The Fine Line Between Fast and Too Fast: Impacts of Updated Regulatory Guidance on Cyber Incident Reporting in the Financial and Critical Infrastructure Sectors

Alison Atkins, U.S. Bank National Association
Jennifer Smestad, Otter Tail Power Company
Robert Cattanach and Jennifer Coates, Dorsey & Whitney LLP

November 17, 2022

CCS | corporate counsel symposium

DORSEY always ahead

Housekeeping

Materials. Session materials and speaker biographies are available on Dorsey.com for download. Search "Corporate Counsel Symposium 2022."

Attendance Sheets are set on tables in this room. If you miss one check at the registration desk.

Q&A. The speakers will not have time to answer audience questions, please contact the speakers or your trusted Dorsey contact.

CLE. A CLE code will be announced for attendees in states that require a Code. **CLE Expected:** AZ, CA, CO, IA, IL, MN, ND, NY, OR, TX, UT, WA, WI.

CCS corporate counsel symposium

DORSEY always ahead

Guest and Dorsey Speakers

Alison Atkins
Assistant General Counsel and Vice President, Cybersecurity,
U.S. Bank National Association

Jennifer Smestad
Vice President, General Counsel, and Corporate Secretary
Otter Tail Power Company

Robert Cattanach
Partner
Dorsey & Whitney LLP

Jennifer Coates
Partner
Dorsey & Whitney LLP

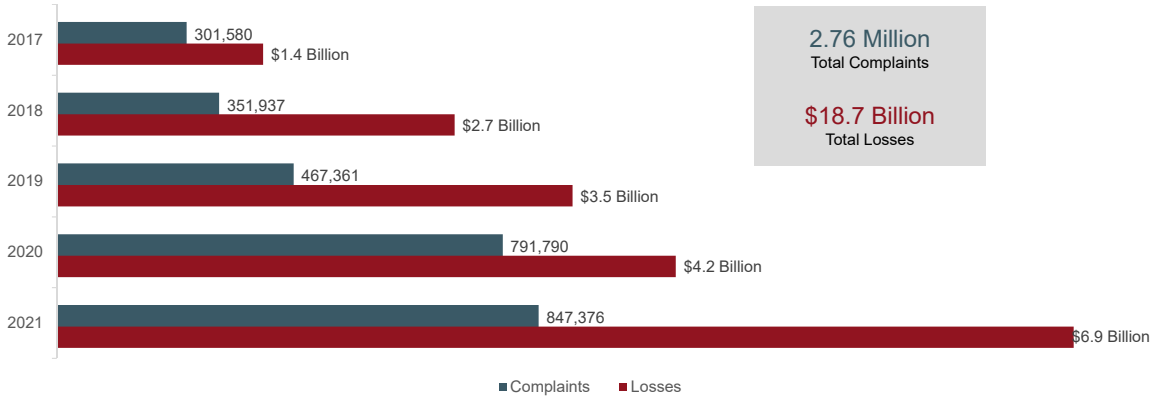
CCS corporate counsel symposium

DORSEY always ahead

Introduction and Background

- **What is driving the federal government to engage?**
  - **Estimates are that cybercrime, if it were a country, would constitute the third largest GDP in the world, after the US and China**
  - **Absence of any meaningful international cooperation prevents extra-territorial reach of law enforcement**
  - **FBI received nearly 850,000 complaints totaling $6.9B in losses in 2021, highest on record**

Complaints and Losses over the Last Five Years



2.76 Million
Total Complaints

$18.7 Billion
Total Losses

*FBI 2021 Internet Crime Report

CCS corporate counsel symposium
DORSEY always ahead

Cybercriminal Targeting Has Pivoted

- **Hacks of large consumer-oriented companies are passé**
- **Ransomware gets all the headlines, but –**
  - **Business Email Compromise (BEC) gets all the money!**
- **Ransomware losses reported to FBI in 2021: $50 Million**
- **BEC losses reported to FBI: $2+ BILLION**
  - **FBI proven effective at recovering fraudulent transfers (RAT)**
  - **Ransomware rarely clawed back**

CCS corporate counsel symposium

DORSEY always ahead

Consequences of Shift to Ransomware and BEC

- No consistency for reporting
  - State breach notification laws may not be triggered
- Lack of critical information sharing within private sector
- Hampers federal regulators and law enforcement: "We can't fight what we can't see"
- Trends likely to continue

CCS corporate counsel symposium

DORSEY always ahead

Why Does This Shift Matter?

- Many ransomware incidents go unreported
  - Reputational harm and embarrassment
  - Some states have prohibited public sector ransomware payments
  - US Department of Treasury's OFAC has issued guidance that ostensibly makes such payments illegal (questionable jurisdictional basis)
- BECs may not trigger classic consumer breach notifications
  - Embarrassment to senior executives that took the bait even more pronounced
- Complicates incident response equation

CCS corporate counsel symposium

DORSEY always ahead

Aggressive Federal Response to Perceived "Underreporting"

- Concerns that companies are exercising too much discretion
- Need for better 'early warning' for national security response
- Inevitable confusion over what is 'material' and 'reportable'
- Risk: shifts the focus of incident response from putting out the fire and finding the cause to C.Y.A.?

CCS corporate counsel symposium

DORSEY always ahead

Result: Cascade of Regulations, Heightened Enforcement, Legislative Initiatives

- Prudential Regulator Guidance Financial Institutions (May 2022)
- Critical Infrastructure Reporting Omnibus Budget Bill (CIRCIA) (June 2022)
- SEC Regulations on Incident Reporting (<u>Proposed</u> February 2022)
  - Wells notice to Solar Winds alleging inadequate cybersecurity disclosures and public statements, inadequate disclosure controls and procedures.
- Langevin Amendment to 2023 NDAA, would create reporting requirements for Systematically Important Entities
  - May not make it in final bill (if there even is one!)

What Is the Intended Effect?

- **Limits private sector discretion for reporting**
  - **Already subject to hindsight enforcement: Uber's CISO convicted of misprision of a felony for classifying a ransom payment as a 'bug bounty' and instructing executives not to report**
- **Accelerates the timeline for reporting incidents:**
  - **Engages federal resources sooner for individual events**
  - **Allows more unified and timely response at the national level**
  - **Promotes awareness of emerging threats and helps agencies react before threats become systemic**

What Are the *Unintended* Consequences?

- **<u>Impossible</u> for most companies to assess an incident within the new timelines**
- **Companies will face a Hobson's choice:**
  - **"Over-report" to avoid potential enforcement**
    - **Creates noise in the system – EU's experience with Article 33**
    - **Questionable 'benefits' of reporting based on incomplete data**
  - ***<u>Or</u>* force private sector to take advantage of opportunities for interpretation**
    - **Need to determine "materiality" before the clock starts**
    - **Could lead to even greater inconsistencies**
- **Shifts priority from responding to assessing nuances of reporting**

Key Features of Prudential Regulator Requirements

- Has a 'computer security incident' caused *actual harm* to the bank's systems or data Confidentiality, Integrity, Availability (CIA)?
- Has it *materially* disrupted or degraded the bank's operations?
- Must notify Prudential Regulator within ***36 hours*** of materiality determination
  - Telephone or email sufficient
    - Typically financial institutions know their regulator personally
    - Can request to keep confidential
  - ***But*** what other obligations will 'confidential' reporting trigger ?!?

Service Providers/Vendors Further Complicate the Equation

- Service Providers must notify the financial institution "as soon as possible."
- Easy default for the vendor: when in doubt, notify your customer
  - Shifts the burden of assessing materiality to a party that doesn't have access to all of the facts
- Creates potentially serious problems for regulated entities
  - ***Don't Assume*** your vendor has reported!
- "Your vendor notified you, why didn't you notify your regulator?"
- May require significant rethinking of notification obligation triggers and timing in 3rd party agreements

CCS corporate counsel symposium

DORSEY always ahead

Standards for Materiality

- ***Ability to carry out its banking operations***, activities, or processes, ***or*** deliver banking products and services to a ***material portion of its customer base***, in the ordinary course of business;
- Business line(s), including associated operations, services, functions, and support, that upon failure would ***result in a material loss of revenue, profit, or franchise value***; or
- Operations, including associated services, functions and support, as applicable, the failure or discontinuance of which would ***pose a threat to the financial stability of the United States***.
- Arguably reconcilable with SEC materiality standards?
- ***But…***

CCS corporate counsel symposium

DORSEY always ahead

Examples *(not included in actual text of regulations)*

- Distributed Denial of Services (DDOS) > 4 hours
- [Service Provider] Widespread system outages – recovery time indeterminable
- Service upgrade causing widespread system outages to customers
- ***Activation of business continuity or disaster recovery plan***
- A ransom malware attack that encrypts a core banking system or backup data

These kinds of events may not be material under more traditional SEC analysis

CCS corporate counsel symposium

DORSEY always ahead

What Are the Practical Implications of the Prudential Regulator Requirements

- Shifts focus on *reporting* when the Incident Response team should be focused on *remediating*
- Reporting and incident response timeline management
- Contract amendments for Banking Service Providers
- Courtesy notifications becoming the rule?

CCS corporate counsel symposium

DORSEY always ahead

Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA)

- Created: Omnibus Budget Bill March 2022
- Applies to "covered entities" – electric sector is 1 of the 16 industries with critical infrastructure
- Report 2 types of cyber events:
  - 72-hour deadline for reporting "covered cyber incidents"
  - 24-hour deadline for reporting ransom payments
    - Vendor "shall advise the impacted covered entity of the responsibilities of the impacted covered entity regarding reporting ransom payments"
- 24 months to promulgate proposed rules (NPRM)
- Final rules must be issued within 18 months of the NPRM

Stated Objectives

- Spot trends
- Share information
- "Render assistance"
- Warn other potential victims
- Not used for enforcement
- *But* can refer to 'appropriate' federal agencies

➢ GOAL: Enhance protection of key national assets – healthcare, financial institutions, nuclear power, electric grid, critical manufacturing, water and telecommunications assets.

Process Underway

- CISA Director's Request For Information (RFI) Sept 12, 2022
  - (60 day submission period expired November 14th);
- 'Listening sessions' (last one Kansas City November 16th)
- What are we learning from the process?
  - Focus of formal comments submitted thus far: Leverage existing reporting methods that are already required through NERC.
  - Be mindful of one-size-fits-all versus actual risk assessments.
  - Different priorities for different critical infrastructure segments
- What could enforcement look like?
  - Subpoenas by CISA.
  - Referral to DOJ for non-compliance.
  - Classic risk of hindsight enforcement ('you should have seen this coming').

Key Elements to Be Developed

- What starts the 72-hour clock?
  - "Reasonable Belief" that a covered/substantial cyber incident has occurred
- Process for submitting reports
- Report contents
  - Supplemental reports
  - What constitutes "substantial new or different information"
- CISA's "balanc[ing] the need for situational awareness with the ability of the covered entity to conduct cyber incident response and investigations"
- Categorical triggers for (some/all?) industry sectors?
- Reconciling with existing triggers and processes (non-public) e.g. NERC-CIP protocols for electric grid

SEC Draft Disclosure Guidelines

- Published March 2022 – ***highly controversial***
  - SEC reopened comment period
  - Likely final rule to be issued in first half 2023
- 4-day deadline to disclose "material" incidents'
- What constitutes "materiality"

  "there is a substantial likelihood that a reasonable shareholder would consider it important in making an investment decision, or if it would have significantly altered the 'total mix' of information made available"

Matrixx Initiatives, Inc. v. Siracusano

What Disclosures Are Necessary?

- **Amend Forms 10-Q and 10-K to update prior disclosures**
- **Include:**
  - **Past and potential impacts**
  - **Status of remediation efforts**
  - **Forthcoming changes to cybersecurity posture.**
- **Also requires disclosure of any series of individually nonmaterial cybersecurity incidents that became material when taken as a whole.**
- **Regulation SK**
  - **Policies and procedures to identify and manage cyber risk.**
  - **Management's role in implementing cyber policies and procedures.**
  - **Board expertise and oversight of cyber risk.**

Examples Provided – *Are They Always Material?*

- **Compromised the confidentiality, integrity, or availability of an information asset (data, system, or network)**
- **Degradation, interruption, loss of control, damage to, or loss of operational technology systems**
- **Unauthorized party accessed, altered, or has stolen:**
  - **Sensitive business information**
  - **Personally identifiable information**
  - **Intellectual property, or**
  - **Information that has resulted in a loss or liability for the registrant**
- **Malicious actor has offered to sell/disclose sensitive data or demanded payment to restore data that was stolen or altered**

Shareholder Litigation and SEC Enforcement

- ***Alphabet*** **1 F. 4th 687 (9th Cir. 2021)**
- **Shareholder claim: Google failed to disclose a substantial breach**
  - **Google Identified cyber incidents *as risks* in prior SEC filings**
  - **Post breach, claimed 'no material changes in risk factors'**
  - **Cited SEC interpretive guidance to support**
- **District Court declined to dismiss, upheld on appeal**
- ***Challenge for plaintiffs*: History establishes that while stock price typically plummets immediately after breach is reported, it eventually rebounds to pre-breach levels before claim goes to trial**

Disclosure Controls: Soft Underbelly for SEC?

- ***In re First Am. Fin. Corp.*** **(C.D. Cal. Sep. 22, 2021)**
  - **Blogger alerts First American to vulnerability**
  - **First American promptly discloses via 8K filing**
  - **IT *was aware* of the vulnerability earlier, *didn't tell management***
  - **Shareholder suit against C-Suite: previous SEC filings misrepresented security status**
  - **Dismissed: No allegation execs had *actual knowledge* of vulnerabilities**
    - **Risk disclosures too vague to create individual liability**
  - **SEC commenced enforcement against First American for inadequate disclosure controls and procedures (*i.e.* management *should have* known)**
  - ***No allegation by SEC that vulnerability was material***
  - **First American settled with SEC for $<500,000**

Conflicting Definitions for "Materiality" Create Significant Challenges

- Advance analysis, planning, and practice will be essential for incident responses
- Prudential Regulators and CISA understandably pressing for lower thresholds for reporting incidents
- No attempt to reconcile with SEC's definition of materiality
  - The SEC's proposed regulations lower materiality threshold
- Potential for conflict and confusion inevitable
- "Just to be safe" vendor notifications will complicate even more

CCS corporate counsel symposium
DORSEY always ahead

Other Challenges Created by Cross Triggers

- When does reporting to Prudential Regulator presumptively trigger SEC filings?
  - Prophylactic trading blackout for executives even if no public SEC filings?
- Same for CISA reporting?
- NY DFS – must be notified if any notice to other supervisory authority
- Utility Regulators – some state PUCs may require reporting
- Contractual obligations to Business Partners

Impacts on Incident Responses

- Critical changes required for IR planning and execution
- Acknowledge: Different notifications for different audiences
  - Document basis of decisions to report, *and not report*
  - Separate decision paths triggered for SEC reporting to ensure consistency
- Cannot address numerous reporting contingencies in real time
- Weighing the consequences
  - Do you disclose if the vulnerability has not been fixed?
- Integrating the communication workflows
- Implications of international obligations

Thank you for attending!

Materials. Session materials and speaker biographies are available on Dorsey.com for download. Search "Corporate Counsel Symposium 2022."

Questions. If you have questions, you may contact the speakers or call on your trusted Dorsey contact.

Legal Notice

This presentation is intended for general information purposes only and should not be construed as legal advice or legal opinions on any specific facts or circumstances. An attorney-client relationship is not created through this presentation.