

· Crypto Currency Claims  
· Lessons from FTX  
· SEC Related Actions

© 2023 Wilson Elser. All rights reserved.

WILSON ELSER

May 23, 2023

Jonathan Meer – Wilson Elser  
Brian Oubre – Nationwide  
Thomas Yohannan - Aon

# Directors and Officers and Cyber

Presentation Part of the 17<sup>th</sup> Annual D&O Insurance ExecuSummit

# Recent Trends with D&O Liability Related to Cyber

- What does a cyber related D&O exposure look like?
- Data Breach Liability Claims
  - Securities Class Actions and Derivative Actions
  - Regulation Compliance for D&Os for Cyber Risks
- Crypto Currency Claims
  - Lessons from FTX
  - SEC Related Actions

# D&Os in the Spotlight

- Claims Against Directors and Officers
  - Common law
    - Duty of Obedience
    - Duty of Loyalty
    - Duty of Diligence
    - Duty of candor
  - Statutory laws, including securities laws
- Business Judgment Rule

# Board Expertise and Reliance on Experts

- A board member does not need to have detailed technical knowledge of a subject area in order to fulfil its duties to a company.
- While board members must acquire a reasonable level of understanding of the company and its level of exposure to cyber (for example) and other risks, they may rely on advice from those individuals in management or outside experts that they reasonably believe do have the expertise necessary to evaluate the company's cyber risks and determine how to protect against cyber intrusions.

# Board Delegation

- A board can delegate some of its responsibilities or certain topical issues, but it does not have to. A board in its entirety can choose to retain authority to address certain issues.
- Often through, a board will give the authority to make a recommendation on a certain topical issues (and in some cases decision making authority) to a committee. For example, in recent years Board have delegated topics like cyber security to an audit committee, a risk committee, a technology committee or a special committee. It is ideal, but not necessary, if the committee or members have some facility for understanding that particular topic. If a committee has a member or members with some expertise in a topic that can be helpful but is not required.
- The board should ensure that there are reasonable reporting structures in place to keep the board adequately informed of any delegated topic/issue.

# Breach of Duty of Oversight/*Caremark*

- After a catastrophic cyber incident, an allegation can be brought that the board of directors breached its duty of oversight
- In order to sustain a claim for breach of the duty of oversight, “the lack of oversight pled must be so extreme that it represents a breach of the duty of loyalty,” which in turn “requires an action (or omission) that a director knows is contrary to the corporate weal.”
- A viable claim may be established only for either “utter failures by directors to impose a system for reporting risk” or for “failure to act in the face of ‘red flags’ disclosed to them so vibrant that lack of action implicates bad faith, *in connection with the corporation’s violation of positive law*”

## Breach of Duty of Oversight/*Caremark* (*continued*)

- Oversight breach claims remain one of the most difficult claims to sustain
- A potential claim is that the board failed to adequately oversee the risk to cybersecurity of a criminal attack
- The criminal acts of third parties means only that the company was the victim of legal violations not the perpetrator.
- The absence of legal duties means that cybersecurity is a business risk, one of many the company faces.
- In order for the cybersecurity-related business risk to give rise to potential board liability, the claimant must establish a “nexus” between the risk and the board.

# Characteristics of a Catastrophic Cyber-Related D&O Securities Claim

A cyber incident does not typically translate into a high severity D&O/Securities claim but for two factors:

1. Cyber security or personal identifiable information is at the core of why the company exists, what the company does, or the services they provide
  - Examples: Equifax or Solarwinds
2. The cyber security incident or event brings down the company
  - a catastrophic ransomware event which takes the company completely offline or renders it inoperable or unable to provide services

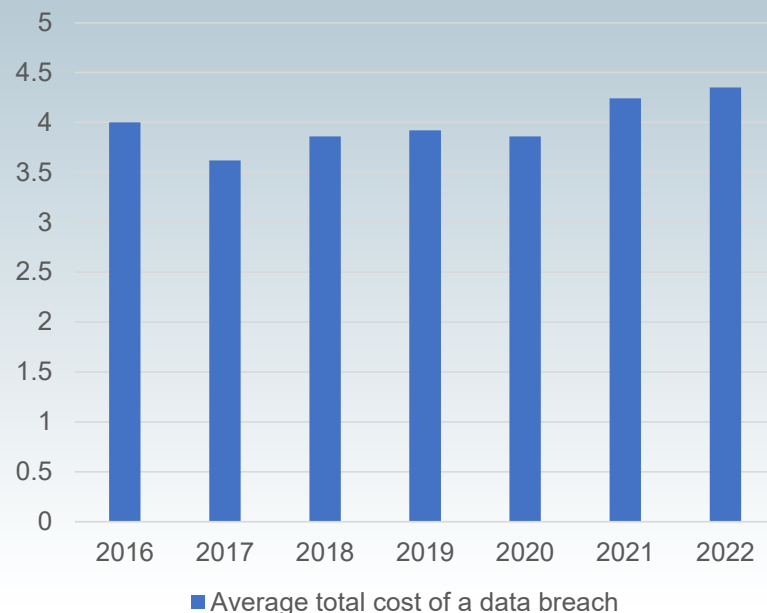


# Litigation Statistics

- Combined filings in the U.S. district courts for civil cases and criminal defendants decreased by 84,137 (down 13 percent) to 385,613 from June 2021 to June 2022. Case filings around same amount as 2018, far off the high of 519,341 in June 2020.
- In 2022, securities filings declined for the third year in a row, with 208 federal court securities class action lawsuits filed. This is a sharp decrease from the 320 federal court filings in 2020 and far less than the 428 new securities class action cases in 2019.
- 2022 had 105 securities settlements for a combined \$3.8 billion.
- In 2022, there was 168 securities claims against public companies.

# Claims in the Cyber Insurance Market

Average total cost a data breach  
(measured in USD million)



Source: IBM Security  
Cost of a Data Breach Report 2022

Average Payouts and Incident  
Costs for SMEs



Source: NetDiligence Cyber  
Claims Study – 2022 Report

# Cybersecurity-Related Litigation

- SEC proposed new rules requiring public companies to promptly disclose material cybersecurity incidents—would impose high burden on corporate boards
- Cyber Incident Reporting for Critical Infrastructure Act (“CIRCA”) signed into law in March, 2022 but will not go into effect until the Cybersecurity and Infrastructure Security Agency (“CISA”) enacts regulations
- SEC has stepped up its enforcement activity in connection with cybersecurity disclosure (*e.g.*, *First American Financial Corp.*, 2021)
- Courts have declined motions to dismiss in suits against SolarWinds and Carbonite corporate boards—but the Delaware Court of Chancery dismissed shareholder derivative allegations following a data breach in the Marriott case

# American Data Privacy & Protection Act ADPPA

- Landmark U.S. federal privacy legislation (pending)
- Follows in the footsteps of GDPR
- Greater protections for PI of U.S. residents
- Consumer bill of rights over their data
- Special protections for Sensitive PI (SPI)
- Disclosure and transparency of collection and use of PI/SPI
- Consumer right to opt-out of sale, targeted ads, transfer of PI
- Timely response to consumer requests to exercise their rights
- Regulatory enforcement (FTC, AGs)
- Private right of action (consumer lawsuits)

# The Biometric Privacy Lawsuit

- Background & Legislative Intent
- Biometric v. Traditional Privacy
- Types of Biometric Privacy Claims
  - Workplace
  - Online
  - Wearables
- Types of Technology
  - Fingerprint Scanners
  - No Contact Temperature Taking Devices
  - Facial Recognition



# Data Breach Claims

- Equifax data breach - Kuhns v. Equifax, Inc., Richard Smith, et al (D. N.D. Georgia)
  - Data breach involved 143 million U.S. Customers personal information
  - D&O's made false or misleading statements regarding Equifax's measures to protect its data and detect security breaches
  - Settled for \$149M in February 2020
- In Re Capital One Customer Data Security Breach Litigation (19-cv-1472) (EDVA)
  - Breach of 100 million customers in US and 6 million in Canada
  - Alleges that Capital One misled its investors by making a series of fraudulent statements that covered up its purported knowledge of the risks that such a data breach could occur, including its failure to maintain adequate data security protections
  - Settled for \$190 million in 2022

## Data Breach Claims (Cont.)

- Lessons from SolarWinds
- *In re: SolarWinds Corp. Securities Litigation*, U.S. District Court, Western District of Texas (21-cv-00138)
  - \$26 million settlement
- *CIL Pension Fund, et al. v. Mike Bingle, et al.*, Delaware Chancery Court (2021-0940)
  - September 6, 2022 dismissal; but currently on appeal

# Data Breach Claims (Cont.)

- Other Litigations

- Block - *Donna Esposito v. Block Inc. et al.*, U.S. District Court, Southern District of New York (22-cv-08636)
- T-Mobile – *Jennifer Baughman v. T-Mobile*, US District Court, Central District of California (23-cv-00477), filed 1/22/23
- Dish Network – *Miguel Jaramillo v. Dish Network Corp, et al*, U.S. District Court, District of Colorado (23-cv-734), filed 3/23/23



# Overview:

## Blockchain / Distributed Ledger Technology

- Electronic database that stores “blocks” of payment and other transactions
- Peer-to-peer system without a central authority or financial intermediary
- Data spread out among various “nodes” on a decentralized network
- Transactions are “validated” by network participants
- Consensus mechanisms
  - Proof of Work (solving mathematical puzzles which requires computational power)
  - Proof of Stake (validators stake capital in the form of crypto assets on the blockchain)
- Immutable record of transaction added to the blockchain
- Blocks stored linearly in chronological order (history of transactions)
- Transparent, trustless, and secure

# The Rise and Fall of FTX

- **FTX companies**

- Founded by SBF in 2019
- Exchange for trading cryptocurrency assets
- Reportedly held \$15B in assets as of 2021
- Terms of Service promised customers control over their assets
- Investment product offering high-yield loans (15% annualized fixed rate, no lockup)
- Issued its own proprietary token (FTT)
- Celebrity endorsements, naming rights to Miami Heat stadium

- **Alameda**

- Founded by SBF (prior to FTX) who served as its CEO until 2021
- Quantitative trading firm specializing in crypto assets
- Engaged in speculative and risky arbitrage trading strategies
- Traded \$600M to \$1B in crypto assets a day at its peak
- One of the largest liquidity providers and market makers in the crypto space

- **Silvergate**

- Founded in 1998 and started providing services for crypto currency users in 2016.
- In 2022, had \$12 billion in deposits including all major crypto exchanges



# The Fall of FTX: Investor Class Actions

- Nationwide Class Action filed against SBF and celebrity sponsors of FTX
- Investors who invested in yield-bearing crypto accounts (YBAs)
- Alleged violations of Florida securities and consumer protection laws
- False and misleading representations to investors
- FTX YBAs are (unregistered) “securities” under the *Howey* Test
  - *SEC v. W.J. Howey Co.*, 328 U.S. 293 (1946)
  - Investment contract is a “security” if it meets 3 criteria:
    - (1) purchaser makes an investment of money or item of value
    - (2) in a common enterprise
    - (3) with the reasonable expectation of profits to be derived from the efforts of others

# U.S. Regulatory Oversight of Crypto Markets: SEC v. Caroline Ellison and Gary Wang

- SEC lawsuit against former CEO of Alameda and CTO of FTX (12/21/22)
- Violations of 1933/1934 Acts re purchase and sale of “securities”
- Scheme to defraud FTX investors by diverting customer funds to Alameda
- Misrepresentations re ownership, control, segregation and use of funds
  - Commingling of FTX customer assets
  - FTX customer funds deposited in bank accounts controlled by Alameda
  - Undisclosed loans by FTX to Alameda
  - Collateralized by illiquid FTT tokens propped up by FTX and Alameda
  - More than \$8B in FTX customer funds siphoned off by Alameda
  - Used to fund Alameda operations, make risky trading bets, pay creditors
  - Misleading “audited” financial statements provided to FTX investors
  - Misleading statements re FTX’s automated 24/7 risk mitigation controls
- Ellison plea agreement with DOJ (12/18/22)

# Silent Crypto Insurance Exposure: Example: D&O coverage for SEC Lawsuit

- *SEC v. SBF* (S.D.N.Y., Dec. 13, 2022)
  - Violations of federal securities laws for investor fraud
  - 90 U.S. investors who invested \$1.1 Billion by purchasing FTX stock
  - Diversion of customer funds and assets
  - False and misleading statements
    - Violations of Terms of Service
    - Customer assets were “safe and secure”
    - FTX employed sophisticated, 24/7 automated risk measures and controls
    - Failure to disclose related-party transfers between FTX and Alameda and commingling of funds
    - Holding large positions in illiquid crypto assets for collateral (incl. FTT tokens)
    - False and misleading (audited) financial statements
  - Relief sought:
    - Disgorgement of ill-gotten gain, Civil monetary penalties
    - D&O bar order
    - Lifetime ban from issuing, purchasing, selling securities and crypto asset securities

# Action against Signature Bank D&Os

**SCHAEFFER V. SIGNATURE BANK**, 23-cv-01921 (E.D.N.Y., March 13, 2023)

- Traditional US Banking markets were reluctant to do business with FTX/Almeida due to the offshore lightly regulated nature of the structure as well as the volatility and security of the digital asset markets. However, beginning in 2018, Signature Bank made a deliberate play to try to attract deposits from cryptocurrency-related businesses
- Signature Bank and its CEO/co-founder Joseph DePaulo CFO Stephen Wyremski in its regulatory filings and public statements represented that :
  - the bank's customer base was fully diversified across nine national middle market lines of business and maintained a high risk-based capital ratio of 10.42 percent, which is in excess of regulatory requirements.
  - Depaulo was quoted on March 9 as re-stating "As a reminder SB does not invest in, does not trade, does not hold, does not custody and does not lend against or make loans collateralized by digital assets"
- Despite the reassurance there was a run on the bank on March 10. After news of SVB's closure began to circulate, depositors at Signature, "panicked" and they began to demand to withdraw their money (over \$10 billion) from Signature.
- The stock which had been trading as high as \$134 in February lost half of its value on March 10 trading at \$70 per share. When it was taken over by the FDIC on March 13, with \$100 billion in assets, it was the third-largest bank failure in history. (Washington Mutual at \$300b+ is still the largest)

# Future Impact of These Claims on D&O Insurers

- Underwriting
  - The issues in these growing areas of business necessitate that Insurers have to understand the risk they are underwriting
- Claims
  - Regulatory Investigations
  - Civil and Governmental Litigation
  - Event-Driven Litigation
  - Shareholder Activism Claims
  - Areas for Future Concern

# Thank you!

**Jonathan E. Meer**

Partner

Wilson Elser

Jonathan.Meer@wilsonelser.com

**Brian Oubre**

Director, Head of Commercial and  
Financial Institutions Claims

Nationwide Insurance

Brian.Oubre@nationwide.com

**Thomas Yohannan**

Vice President – Strategy & Partner Programs

Aon Cyber Solutions

Thomas.Yohannan@aon.com