Red Sky at Morning: A Look at Responsible Corporate Officer Liability for Cyber Breaches

Kara D. Schwee

I. INTRODUCTION

The Responsible Corporate Officer Doctrine [hereinafter the "Doctrine"] was created to promote the public welfare by holding corporate officers responsible as "least-cost avoiders"—the parties with the ability to prevent a problem at the lowest cost.[1] This

1. *In re* Dougherty, 482 N.W.2d 485, 489 (1992) (discussing the Doctrine's application to public welfare offenses); *see also* Giuseppe Dari-Mattiacci & Nuno Garoupa, *Least-Cost Avoidance: The Tragedy of Common Safety*, 25 J.L. ECON. & ORG. 235, 235 (2009) (defining least cost avoider as "the party who could have prevented the accident at the lowest cost").

statutory-based Doctrine is generally used when an organization violates a public welfare statute.[2] An officer may be held liable even if the officer had no knowledge of, nor involvement in, the wrongful actions of their associates.[3]

As a strict liability doctrine, the Doctrine was initially limited in its focus.[4] Now its scope is expanding further within the healthcare industry.[5] Data security breaches, increasingly commonplace, are becoming a minefield for corporate officers under the Doctrine.

This Note will: (I) provide an overview of the Responsible Corporate Officer Doctrine; (II) discuss healthcare data breaches; (III) examine implications of holding corporate officers responsible for data breaches under the Doctrine; and (IV) analyze the application of the Doctrine to healthcare data breaches. In addition, this Note will show that a legislative solution is needed now that data security breaches are on course to become a trigger of the Doctrine. This will promote corporate education and implementation of compliance programs as a way for corporate officers to avoid civil and criminal liability because of a data breach.

II. THE RESPONSIBLE CORPORATE OFFICER DOCTRINE

The Doctrine holds corporate officers responsible for their corporations' unlawful actions—subjecting officers to both civil liability and criminal convictions for misdemeanors and felonies.[6] In the civil context, the idea that an individual—for instance, a corporate officer—is liable for torts committed is generally accepted regardless of whether the corporate officer's corporation is also liable for the torts.[7] A corporate officer can also be criminally responsible without analysis of mens rea.[8] The "harsh but also narrow and lenient"[9] Doctrine, read broadly, holds that a corporate officer can be held personally liable for the crimes of a subordinate.[10] Corporate officers find the Doctrine

2. JAMES D. COX & THOMAS LEE HAZEN, TREATISE ON THE LAW OF CORPORATIONS § 8:22 (2019) ("The doctrine . . . is generally limited to violations of certain 'public welfare' or 'regulatory' statutes that encompass a strict liability standard.").

3. United States v. Dotterweich, 320 U.S. 277, 281 (1943).

4. *Dotterweich* articulates a limiting principle which showed that corporate officers bear a 'responsible relationship' to, or have a 'responsible share' in, violations." United States v. Park, 421 U.S. 658, 672 (1975).

5. Jane Kim, *Staying Responsible within the Healthcare Industry in the Era of the Responsible Corporate Officer Doctrine*, 14 IND. HEALTH L. REV. 129, 138 (2017) (discussing the Doctrine's 2013 extension to "third-party contractors (distributors) carrying responsibility for the actions of the manufacturers" and arguing the Doctrine "now appears to have a very wide reach indeed").

6. *Id.* at 130.

7. 3A WILLIAM MEADE FLETCHER ET AL., FLETCHER CYCLOPEDIA OF THE LAW OF PRIVATE CORPORATIONS § 1135 (perm. ed., rev. vol. 2018) [hereinafter FLETCHER CYCLOPEDIA] ("It is the general rule that an individual is personally liable for all torts the individual committed, notwithstanding that the person may have acted as an agent or under directions of another. This rule applies to torts committed by those acting in their official capacities as officers or agents of a corporation. It is immaterial that the corporation may also be liable.") (internal citations omitted).

8. Meant to protect the public from harm, "strict liability criminal provisions" in public statutes create the possibility that "a corporate official can be criminally responsible without proof of his knowledge of a violation." COX & HAZEN, *supra* note 2.

9. Samuel W. Buell, *The Responsibility Gap in Corporate Crime*, 12 CRIM. L. & PHIL. 471, 484 (2018).

10. Craig S. Lerner, *The Trial of Joseph Dotterweich: The Origins of the "Responsible Corporate Officer" Doctrine*, 12 CRIM. L. & PHIL. 493, 494 (2018) (broadly defining the Doctrine as one in which a corporate officer can be held personally liable "for the criminal act of a subordinate if the officer was, in some indefinite way, able

disconcerting because no proof of intent or conscious wrongdoing is necessary to establish liability for a criminal offense.[11]

One of the primary debates regarding the Doctrine is its lack of a mens rea element.[12] Long used to assess wrongdoers' criminality,[13] the term "mens rea" refers to "[t]he state of mind that the prosecution, to secure a conviction, must prove that a defendant had when committing a crime; criminal intent or recklessness."[14] The mens rea element protects many of our societal beliefs regarding personal freedom and responsibility.[15]

Convicting for public welfare violations without mens rea began with a series of cases involving "the sale of impure or adulterated food"[16] and the regulation of alcohol.[17] The Doctrine generally applies to "public welfare" statute violations.[18] This concept of public welfare offenses first appeared in 1933.[19] However, it was a 1952 case—*Morisette v. United States*—in which the Court explained that individuals could be held criminally responsible for some public health and welfare offenses without proving mens rea.[20]

Rather than simply punishing criminal misbehavior, which typically requires a mens

---

to prevent the violation").

11. Kim, *supra* note 5, at 138 ("[N]o proof of intent or actual knowledge of the violations by the Corporate Officials to establish their guilt for the misdemeanor offense") (quoting Michael Friedman et al. v. Sebelius et al., 2010 WL 2519161, at *12 (D.D.C. 2010))).

12. Andrew C. Baird, *The New Park Doctrine: Missing the Mark*, 91 N.C. L. REV. 949, 972 (2013) ("One of the primary debates surrounding the use of the Park doctrine is its capacity to subject individuals to an exclusion or debarment via strict liability.").

13. Francis Bowes Sayre, *Public Welfare Offenses*, 33 COLUM. L. REV. 55, 56 (1933) ("[T]he *mens rea* is as vitally necessary for true crime as understanding is necessary for goodness. To inflict substantial punishment upon one who is morally entirely innocent, who caused injury through reasonable mistake or pure accident, would so outrage the feelings of the community as to nullify its own enforcement."); *see also* United States v. Cordoba-Hincapie, 825 F. Supp. 485, 489–90 (E.D.N.Y. 1993).

14. *Mens Rea*, BLACK'S LAW DICTIONARY (7th ed. 2000).

15. *Cordoba-Hincapie*, 825 F. Supp. at 496 (explaining that the element of mens rea "guards beliefs deeply held within our traditions of individual freedom, responsibility and duty").

16. Sayre, *supra* note 13, at 57–64 ("The offense of selling adulterated or impure food, which today is the typical example of a crime not requiring *mens rea*, was held by English courts before the middle of the nineteenth century, like other crimes, not punishable without proof of guilty intent" until "*Regina v. Woodrow* in 1846[,]" when a tobacco dealer with "no knowledge or cause to suspect" he was selling impure tobacco was held liable for possession of adulterated tobacco.) (internal citations omitted). The development of strict liability welfare laws in America started "[i]n *Barnes v. State*, decided in Connecticut in 1849." *Id.* at 63. The similar timeframe of the development of this new class of cases for which no mens rea be proved "strongly indicates that the movement has been not merely an historical accident but the result of the changing social conditions and beliefs of the day." *Id.* at 67. The shift shows a cultural desire to emphasize "protection of public and social interests" over individual interests, and the use of criminal law to enforce "a new type of twentieth century regulatory measure involving no moral delinquency." *Id.*

17. *Id.* at 62–64 (discussing the development of strict liability welfare laws in America, beginning with "*Barnes v. State*, decided in Connecticut in 1849").

18. COX & HAZEN, *supra* note 2, at § 8:22 (explaining the Doctrine's narrow application to strict liability public welfare statutes).

19. *See* Sayre, *supra* note 13, at 56 (coining the phrase "Public Welfare Offenses").

20. Morissette v. United States, 342 U.S. 246, 253–54 (1952) ("Wide distribution of goods became an instrument of wide distribution of harm when those who dispersed food, drink, drugs, and even securities, did not comply with reasonable standards of quality, integrity, disclosure and care."); *see also* United States v. Dotterweich, 320 U.S. 277, 280 (1943) (discussing a strengthening of FDA regulations).

rea element,[21] public welfare statutes were put into place to protect the public.[22] Public welfare statutes impose greater obligations on individuals,[23] levying strict liability upon violators of these laws.[24] Many detailed regulations have increased the duty of care for those with the power to impact the welfare of the public.[25] One such public welfare statute is the Federal Food, Drug, and Cosmetic Act (FDCA) which regulates a variety of products that affect public welfare.[26]

The strict liability nature of the Doctrine can lead to unexpected results. For example, a corporate officer can take steps that enable them to avoid civil liability, yet a case may still result in the corporate officer's criminal responsibility under the Doctrine.[27]

A. Liability Under the Doctrine

In the Doctrine context, "responsible" means that the individual is responsible for the corporation, rather than for the misconduct.[28] The elements courts use to determine whether someone violates the Doctrine are: (1) the individual has an influence on corporate policies or activities; (2) there is a nexus between the individual's position and the violation; and (3) the individual's actions or inactions facilitate the violations.[29]

---

21. "Generally speaking, prosecutors are required to prove that a defendant had the specific intent or purpose to commit a crime that is inherently evil or wrongful, or *malum in se*, such as robbery or assault." WASH. LEGAL FOUND., FEDERAL EROSION OF BUSINESS CIVIL LIBERTIES 1-1 (2008), https://s3.us-east-2.amazonaws.com/washlegal-uploads/upload/WLF%20timeline.pdf [https://perma.cc/RL6M-L43Y] (emphasis in original).

22. Public welfare statutes "encompass a strict liability standard" as a result of shifting "the traditional bases for criminalizing conduct . . . from punishment of misbehavior to protection of the public from harm." COX & HAZEN, *supra* note 2, at § 8:22.

23. Public welfare statutes are influential because "the legislature and the judiciary impose greater obligations on individuals when public health and welfare are at stake." Noël Wise, *Personal Liability Promotes Responsible Conduct: Extending the Responsible Corporate Officer Doctrine to Federal Civil Environmental Enforcement Cases*, 21 STAN. ENVTL. L.J. 283, 292–93 (2002); *see also Dotterweich*, 320 U.S. at 280–81.

24. The violation of a public welfare statute "is considered a 'public welfare offense,'" which does not require a mens rea element. WASH. LEGAL FOUND., *supra* note 21, at 1–7.

25. *Morissette*, 342 U.S. 246 at 254 ("[Public welfare] dangers have engendered increasingly numerous and detailed regulations which heighten the duties of those in control of particular industries, trades, properties or activities that affect public health, safety or welfare.").

26. Sasha Ivanov, *When the Punishment Does Not Fit the Crime: Exclusions from Federal Health Care Programs Following Convictions under the Responsible Corporate Officer Doctrine*, 84 GEO. WASH. L. REV. 776, 782 (2016) ("Violations of the FDCA, which regulates food, drugs, medical devices, and other products that affect public health and safety, are widely considered to be public welfare offenses.").

27. Kim, *supra* note 5, at 132 ("[W]hile a [corporate officer] will be safe from *civil* liability by operation of the 'business judgment rule' when he or she fulfills his or her . . . oversight duties, the [corporate officer] can be held *criminally* responsible by operation of the RCO doctrine *even if* he or she did not know that company employees had violated public welfare laws.") (quoting Michael E. Clark, *The Responsible Corporate Officer Doctrine: A Re-Emergent Threat to General Counsel and Corporate Officers*, 14 J. HEALTH CARE COMPLIANCE 5, 6 (2012))).

28. "The word 'responsible' in the doctrine's name does not mean that the individual is responsible for the *misconduct*, but . . . that the individual is responsible for the *corporation*." Kevin M. LaCroix, *More About the Responsible Corporate Officer Doctrine*, D&O DIARY (Mar. 8, 2010), https://www.dandodiary.com/2010/03/articles/corporate-governance/more-about-the-responsible-corporate-officer-doctrine [https://perma.cc/2EEK-ERDW].

29. "An individual may be found personally liable under [the Doctrine] under the following circumstances: (1) the individual must be in a position of responsibility that allows the person to influence corporate policies or activities; (2) there must be a nexus between the individual's position and the violation in question such that the

The first element of liability under the Doctrine requires that the individual is in a position of responsibility such that the individual has an influence on corporate policies or activities.[30] An individual who acts on authority entrusted to them by their company is in a position of responsibility.[31] Such individuals may include corporate officers[32] and directors.[33]

The second element of liability under the Doctrine requires a nexus between the individual's position and the violation.[34] A possible nexus between position and violation is a corporate officer's failure to act on notice of criminal misconduct (regardless of whether they had the notice or simply should have had the notice).[35]

The final element of liability under the Doctrine is the individual's actions or inactions facilitate the violations.[36] This is the element that should offer the most "peace of mind" to corporate officers.[37] This element ensures that, in addition to their position within the company and that position's responsibility for the actions within the company, the violation was "actually allowed" by the corporate officer.[38]

B. History and Development of the Doctrine

The Doctrine developed through a series of cases. Initially used in the criminal law context, courts have applied the Doctrine when considering corporate officers' civil liability in situations where their corporation violates a public welfare statute and the violation is the proximate cause of a plaintiff's harm.[39]

1. Early Case Development

The three primary cases involved in the Doctrine's early development are *United States v. Balint*, *United States v. Dotterweich*, and *United States v. Park*.

---

individual could have influenced the corporate actions that constituted the violations; and (3) the individual's actions or inactions facilitated the violations." FLETCHER CYCLOPEDIA, *supra* note 7; *see, e.g.*, Reed v. Reid, 980 N.E.2d 277 (Ind. 2012).

30. FLETCHER CYCLOPEDIA, *supra* note 7.

31. A person is in a position of responsibility if they "exercis[e] authority and supervisory responsibility reposed in them by a business organization . . . ." United States v. Park, 421 U.S. 658, 658–59 (1975).

32. "In corporate law, the term refers esp. to a person elected or appointed by the board of directors to manage the daily operations of a corporation, such as a CEO, president, secretary, or treasurer." *Officer*, BLACK'S LAW DICTIONARY (7th ed. 2000).

33. *See generally* COX & HAZEN, *supra* note 2 (discussing criminal liability).

34. People v. Roscoe, 169 Cal. App. 4th 829, 839 (2008) (explaining the second element of the Doctrine, that "there must be a nexus between the individual's position and the violation in question such that the individual could have influenced the corporate actions which constituted the violations").

35. *See* United States v. Y. Hata & Co., 535 F.2d 508, 511 (9th Cir. 1976) (explaining that the corporation was aware of the bird infestation problem); United States v. Starr, 535 F.2d 512, 515 (9th Cir. 1976) (evaluating a mouse infestation of a warehouse).

36. *See In re* Dougherty, 482 N.W.2d 485, 490 (Minn. Ct. App. 1992) (stating the third element of the Doctrine, "the individual's actions or inactions facilitated the violations").

37. Valorie Cogswell, *Catching the Rabbit: The Past, Present, and Future of California's Approach to Finding Corporate Officers Civilly Liable Under the Responsible Corporate Officer Doctrine*, 33 ENVIRONS ENVTL. L. & POL'Y J. 343, 365 (2010).

38. *Id.* at 365 (This final element "embodies the notion that the corporate individual must . . . not only have a theoretical responsibility for, or connection to, the violation at issue, but that this individual's actions or inactions actually allowed these violations to occur."); *see also In re Dougherty*, 482 N.W.2d at 490.

39. The Doctrine also applies to administrative actions. Clark, *supra* note 27, at 5.

In 1922, the first case to hint at the Doctrine was *United States v. Balint*—a criminal case.[40] In *Balint*, the defendants were accused of violating the Narcotic Act of December 17, 1914.[41] Specifically, the defendants were charged with the unlawful sale of derivatives of opium and coca leaves.[42]

The defendants protested, saying the allegation had not charged that the defendants had sold the illegal drugs "knowing them to be such."[43] Although mens rea is not an element of the offense according to the Narcotic Act statute itself, the customary common law rule assumed mens rea was a requirement in the indictment of every crime—including, the defendants argued, the offense against the Narcotic Act.[44]

However, the Court responded that the common law element of mens rea would be "modified" in this and other situations in which the purpose of a statute "would be obstructed" by the requirement of mens rea.[45] The *Balint* Court explained that the focus of Section 2 of the Narcotic Act is already to "require every person dealing in drugs to ascertain at his peril" whether the statute applies to the drugs they are selling and, if it does apply, to apply it correctly.[46] The Court further explained that removing the mens rea element in cases involving a public welfare offense with misdemeanor repercussions would not violate due process.[47]

The Doctrine as we know it originated in *United States v. Dotterweich*, in which a pharmaceutical company and its president were charged with violating the Federal Food, Drug, and Cosmetic Act (FDC Act).[48] Specifically, the company and its president were charged with purchasing pharmaceuticals from manufacturers, repackaging the

40. Kim, *supra* note 5, at 136 ("The RCOD's roots can be traced to the 1922 *Balint* case, which involved an indictment of an individual for a violation of the Narcotic Act.") (citing Ronald M. Broudy, *RCRA and the Responsible Corporate Officer Doctrine: Getting Tough on Corporate Offenders by Sidestepping the Mens Rea Requirement*, 80 KY. L.J. 1055, 1057 (1991); United States v. Balint, 258 U.S. 250, 250 (1922)).

41. *Balint*, 258 U.S. at 251 ("Defendants . . . were indicted for a violation of the Narcotic Act of December 17, 1914, 38 Stat. 785, 786 (Comp. St. § 6287g-6287q).").

42. *Id.* ("The indictment charged them with unlawfully selling to another a certain amount of a derivative of opium and a certain amount of a derivative of coca leaves, not in pursuance of any written order on a form issued in blank for that purpose by the Commissioner of Internal Revenue, contrary to the provisions of section 2 of the act.").

43. The defendants protested, saying the allegation "failed to charge that they had sold the inhibited drugs knowing them to be such." *Id.*

44. "[T]he general rule at common law was that the [mens rea] was a necessary element in the indictment and proof of every crime, and this was followed in regard to statutory crimes even where the statutory definition did not in terms include it." *Id.* at 251–52.

45. *Id.* at 252 ("[T]here has been a modification of this view in respect to prosecutions under statutes the purpose of which would be obstructed by such a requirement.").

46. *Balint*, 258 U.S. at 254.

47. Wise, *supra* note 23, at 305 (explaining the Balint Court's point "that due process was not violated when what was essentially a strict liability standard was imposed upon a defendant in a criminal case if the defendant committed a public welfare offense that had misdemeanor, and not felony, repercussions"); *see, e.g.*, *Balint*, 258 U.S. at 252 ("It has been objected that punishment of a person for an act in violation of law when ignorant of the facts making it so, is an absence of due process of law. But that objection is considered and overruled . . . . [We] held that in the prohibition or punishment of particular acts, the state may in the maintenance of a public policy provide 'that he who shall do them shall do them at his peril and will not be heard to plead in defense good faith or ignorance.' Many instances of this are to be found in regulatory measures in the exercise of what is called the police power where the emphasis of the statute is evidently upon achievement of some social betterment . . . ."); *see also* FLETCHER CYCLOPEDIA, *supra* note 7 (in the civil context, the Doctrine "applies to public welfare offenses that impose strict liability by plain language and intent").

48. *See generally* United States v. Dotterweich, 320 U.S. 277 (1943).

pharmaceuticals with their label, and introducing the mislabeled pharmaceuticals into interstate commerce.[49] Defense for *Dotterweich* noted that "Dotterweich was not intimately involved in day-to-day operations" and raised questions "of good faith."[50]

In *Dotterweich*, the Court warned that the class of people who could be held liable is too vague to define under the Doctrine.[51] The Court acknowledged the definition of "person" includes a corporation, but reasoned a corporation does not act on its own.[52] According to the *Dotterweich* Court, it does not make sense to hold only a corporation liable.[53] Instead, the corporation was acquitted while the officer was held liable—even though the officer had no personal knowledge of the criminal activity occurring at his company.[54]

The *Dotterweich* Court's decision asserted that

> 1) when legislation is enacted to protect the public health or welfare, 2) a corporate employee who holds a position of responsibility may be penalized for violating the tenets of that legislation, 3) even though he or she did not participate in the prohibited conduct or have personal knowledge of the violations, 4) if that individual could have, within the scope of his or her responsible position for the corporation, prevented the violation, and failed to do so.[55]

Although *Dotterweich* involved a criminal prosecution, it established a foundation for criminal and civil cases involving the Doctrine.[56] The *Dotterweich* Court explains the identification of similarities between an officer and their corporation.[57] The *Dotterweich* Court also recognized that the purpose of the statute should be used to clarify in situations that require "extensive statutory interpretation."[58]

In *Balint* and *Dotterweich*, the Court held that the legislative intent for public welfare laws was to balance the possibility of penalizing an innocent person against the possibility of exposing the innocent public to danger.[59] Protecting the innocent public, the Court concluded, was more important.[60]

---

49. *Id.* at 278.

50. Lerner, *supra* note 10, at 495, 507.

51. Cogswell, *supra* note 37, at 353 (discussing "the Supreme Court's provocative warning in *Dotterweich* that '[i]t would be too treacherous to define or even to indicate by way of illustration the class of employees which stands in . . . responsible relation' to the public welfare") (citing *Dotterweich*, 320 U.S. at 285).

52. *Dotterweich*, 320 U.S. at 281 (holding that while the statute 49 U.S.C.A. § 303 includes "person" in its definition of "corporation," "the only way in which a corporation can act is through the individuals who act on its behalf").

53. *Id.*

54. *See generally id.*

55. Wise, *supra* note 23, at 302 (citing *Dotterweich*, 320 U.S. at 280–84).

56. Cogswell, *supra* note 37, at 352 (explaining that although *Dotterweich* "involved a criminal prosecution under the [FDC Act], it establishes two fundamental concepts that lay the groundwork for nearly all RCOD cases, both civil and criminal").

57. *Id.* (stating that, in *Dotterweich*, "[t]he Supreme Court took great care to distinguish between a successful RCOD prosecution and 'the rare case where the corporation is merely an individual's alter ego'"); *see, e.g.*, *Dotterweich*, 320 U.S. at 282.

58. Cogswell, *supra* note 37, at 352 (explaining the *Dotterweich* Court "recognized that in cases calling for extensive statutory interpretation, the purposes of the statute 'should infuse construction of the legislation'") (quoting *Dotterweich*, 320 U.S. at 280).

59. *Dotterweich*, 320 U.S. at 281 (explaining that legislation that uses penalties as a means of regulation put the burden of acting "at hazard" on a person "in responsible relation to" endangering the public welfare).

60. United States v. Balint, 258 U.S. 250, 254 (1922) (the Supreme Court holding that "Congress weighed

More than 30 years after *Dotterweich,* the Doctrine developed further in *United States v. Park* by holding that a corporate officer cannot use delegation as a defense to the Doctrine.[61] The defendant in *United States v. Park* was the president of Acme Markets—a large national food chain company—that was being sued for sanitation concerns after evidence of rodents was discovered in his warehouse.[62]

As the President of Acme Markets, John R. Park was "generally unaware" of violations concerning the safety of his company's product.[63] While he was aware of the sanitation issues at his company,[64] he testified that specific responsibilities were delegated through the company's organizational structure.[65] Operational functions of the company—including sanitation—were assigned to subordinate employees working at the company.[66] Park testified in his defense that he had "great confidence" in these employees.[67] While the employees responsible for sanitation were generally under his direction, Park testified that he did not believe he could do any more to rectify the sanitation issues.[68] Both Park and his company, however, had received two letters regarding the rodents in the warehouse.[69]

The Court held that as the president of the company, Park had the ability and failed to either prevent or correct the sanitation issues.[70] The Court also mentioned that because the FDA had advised Park about the sanitation issues, Park was on notice that his employees were not adequately handling the sanitation issues on their own.[71]

---

the possible injustice of subjecting an innocent seller to a penalty against the evil of exposing innocent purchasers to danger from the drug, and concluded that the latter was the result preferably to be avoided").

61. United States v. Park, 421 U.S. 658, 671, 677–78 (1975); *see also* Cogswell, *supra* note 37, at 354 (stating "*Park* held that delegation of duties will not relieve RCOD liability").

62. *Park*, 421 U.S. at 658 ("Acme Markets, Inc., a large national food chain, and respondent, its president, were charged with violating § 301(k) of the Federal Food, Drug, and Cosmetic Act (Act) in an information alleging that they had caused interstate food shipments being held in Acme's Baltimore warehouse to be exposed to rodent contamination.").

63. "As President and CEO of a nationwide retail food chain with over 35,000 employees, almost 900 stores, and 16 warehouses, Mr. Park was generally unaware of the food safety violations." Brian T. McGovern et al., *The Responsible Corporate Officer Doctrine in the Wake of DeCoster*, MARTINDALE-HUBBELL (June 6, 2017), https://www.martindale.com/health-care-law/article_Cadwalader-Wickersham-Taft-LLP_2246738.htm (citing *Park*, 421 U.S. at 661, 663).

64. *Park*, 421 U.S. at 658 ("Evidence was admitted over respondent's objection that he had received a Food and Drug Administration (FDA) letter in 1970 concerning insanitary conditions at Acme's Philadelphia warehouse.").

65. *Id.* at 663 (Park "testified that, although all of Acme's employees were in a sense under his general direction, the company had an 'organizational structure for responsibilities for certain functions' according to which different phases of its operation were 'assigned to individuals who, in turn, have staff and departments under them.' He [Park] identified those individuals responsible for sanitation.").

66. *Id.* (noting Park "identified those individuals responsible for sanitation").

67. *Id.* at 677 ("[Park] testified in his defense that he had employed a system in which he relied upon his subordinates, and that he was ultimately responsible for this system. He testified further that he had found these subordinates to be 'dependable' and had 'great confidence' in them.").

68. Park "stated that he did not 'believe there was anything [he] could have done more constructively than what [he] found was being done.'" *Id.* at 663–64.

69. *Park*, 421 U.S. at 661, 663.

70. *Id.* at 673–74 (holding that Park "had, by reason of his position in the corporation, responsibility and authority either to prevent in the first instance, or promptly to correct, the violation complained of, and that he failed to do so").

71. *Id.* at 678 (noting that following his receipt of the letter from the FDA, Park "was on notice that he could not rely on" his employees "to prevent or correct [un]sanitary conditions" at his company).

2. Recent Cases and Trends

Recent cases have continued to shape the boundaries of liability and penalties under the Doctrine. Four high-profile cases include *United States v. Purdue Frederick Co., Inc.*, *United States v. Marc S. Hermelin*, *United States v. Huggins*, and *United States v. DeCoster*.

After three decades of relative silence,[72] the Responsible Corporate Officer Doctrine experienced a revival starting in 2007 with the Purdue Frederick Company (Purdue)'s conviction of felony misbranding OxyContin.[73] The government alleged that Purdue had encouraged the use of marketing that "defrauded and misled the public" to promote the use of OxyContin.[74] The fraudulent marketing messages, primarily directed toward healthcare providers, downplayed the medication's potential for abuse.[75]

In addition to prosecuting Purdue, the government also prosecuted three of Purdue's responsible corporate officers—the CEO, the executive vice president and chief legal officer, and the chief scientific officer[76]—for Purdue's misconduct. The government was unable to show that the corporate officers knew of, or participated in, the company's misconduct.[77] Regardless, the three corporate officers pleaded guilty to the misdemeanor drug misbranding charge[78] for their failure to prevent their company's misbranding.[79]

Purdue paid $600 million in monetary sanctions and fines.[80] The corporate officers paid millions of dollars in fines[81] and were later excluded from participation in federal healthcare programs (Medicare and Medicaid) for twelve years.[82]

---

72. *See generally* Thomas Mortell & Michelle Gustavson, *The Resurgence of the Responsible Corporate Officer Doctrine*, 55 THE ADVOCATE 32 (2012), https://www.yumpu.com/en/document/read/8763321/the-advocate-june-july-2012-idaho-state-bar-idahogov/5 [https://perma.cc/6C3B-BX33]; *see also* Baird, *supra* note 12, at 951 ("The doctrine fell out of use for nearly two decades after its genesis in the 1970s, but has recently reemerged as a potent . . . regulatory enforcement tool.").

73. Jennifer M. Green, *Corporate Torts: International Human Rights and Superior Officers*, 17 CHI. J. INT'L L., 447, 507 (2017) ("In what has been labeled a 'resurgence' of the RCO doctrine, in 2007, the Department of Justice brought charges against three officers for the misbranding and fraudulent marketing of OxyContin."); *see also* Ivanov, *supra* note 26, at 778 ("In 2007, Purdue Frederick Company, a subsidiary of the drug company Purdue Pharma ('Purdue'), was convicted of felony fraudulent misbranding of the pain medication OxyContin.") (citing Friedman v. Sebelius, 686 F.3d 813, 816 (D.C. Cir. 2012)).

74. The allegations were that Purdue had "defrauded and misled the public through its marketing and promotion of OxyContin" and "presented evidence that Purdue trained sales representatives and sponsored trainings to disseminate false messages to encourage OxyContin use." McGovern, *supra* note 63.

75. The misbranding charges were that Purdue had, for over five years, "marketed and promoted OxyContin as less addictive, less subject to abuse and diversion, and less likely to cause tolerance and withdrawal than other pain medications[.]" United States v. Purdue Frederick Co., 495 F. Supp. 2d 569, 571 (W.D. Va. 2007).

76. *Id.* at 570 n.2 ("Friedman is the former president and CEO of Purdue, Udell is the executive vice president and chief legal officer, and Goldenheim is the former chief scientific officer.").

77. Ivanov, *supra* note 26, at 778 ("Unlike traditional criminal liability, which requires a culpable mental state, appellants argued here that there was no evidence that the officers knew of, or participated in, any of the company's wrongdoing.").

78. *Purdue*, 495 F. Supp. 2d at 570 ("The individual defendants, Michael Friedman, Howard R. Udell, and Paul D. Goldenheim, have pleaded guilty to the misdemeanor charge of misbranding, solely as responsible corporate officers.").

79. Friedman v. Sebelius, 686 F.3d 813, 816 (D.C. Cir. 2012).

80. *Purdue*, 495 F. Supp. 2d at 572.

81. *Id.* at 573.

82. *Sebelius*, 686 F.3d at 816 ("Based upon their convictions, the Secretary of Health and Human Services later excluded the individuals from participation in Federal health care programs for 12 years, pursuant to 42

In 2011, the government alleged that morphine sulfate tablets shipped into interstate commerce by KV Pharmaceutical contained a higher dose and more active ingredients than indicated on their labels.[83] Under the FDCA, a company's misleading labeling of the type that was exhibited by KV Pharmaceutical constitutes misbranding.[84] Hermelin, the CEO of KV Pharmaceutical, did not know about his company's misconduct.[85] Regardless, Hermelin was charged under the Doctrine, because he "had the power, authority, and responsibility" to both prevent and resolve such misbranding issues, yet he did neither.[86] As a result, Hermelin was ordered to pay $1.9 million in fines.[87]

The first prison sentence for a Doctrine violation came later in 2011 when the government charged Synthes with "off-label" use of a bone cement product that had only been approved by the U.S. Food and Drug Administration for specific usage.[88] Multiple patients died as a result of Synthes' unauthorized usage of the product.[89]

Four of the company's former corporate officers were charged with a misdemeanor under the Doctrine.[90] This case stands out from previous strict liability Doctrine cases because its prosecution contended the corporate officers acted knowingly.[91] In addition to payment of a small fine, Michael D. Huggins, the president of Synthes, was sentenced to nine months' imprisonment under the Doctrine.[92] However, based on the substantial evidence that Huggins acted knowingly, he may have been convicted of fraudulent misbranding had his case gone to trial.[93]

In *United States v. DeCoster*, the Eighth Circuit U.S. Court of Appeals considered whether a defendant needs to know they violated a statute before they can be subject to penalties of the statute (and "whether *Park* and its precursor, *United States v. Dotterweich*, should be overruled").[94]

U.S.C. § 1320a–7(b).").

83. United States v. Hermelin, No. 4:11CR00085 ERW, 2011 WL 841001, at *2 (E.D. Mo. Mar. 11, 2011).

84. *Id.*

85. *Id.*

86. *Id.* at *1 ("By virtue of his role at KV, Hermelin had the power, authority, and responsibility to prevent drug manufacturing problems in the first instance and promptly correct any drug manufacturing problems that did occur.").

87. Roscoe C. Howard Jr. & Leasa Woods Anderson, *Trends in Responsible Corporate Officer Doctrine under FDCA*, LAW360 (Dec. 14, 2015, 1:11 PM), https://www.law360.com/articles/737403/trends-in-responsible-corporate-officer-doctrine-under-fdca [https://perma.cc/NMY2-ZYFN].

88. *Id.* ("Later in 2011, in United States v. Synthes Inc., we saw the first prison terms for RCO violations. In Synthes, the government charged the company with conducting unauthorized tests of its bone cement on about 200 spinal surgery patients—three patients died on the table. The bone cement product had U.S. Food and Drug Administration approval for use in the arm, but not in the spine. Synthes was charged with training surgeons to use it "off-label" so the company could gather data for expanded use.").

89. *Id.*

90. *Id.* (stating "four former Synthes executives pleaded guilty or 'no contest' to a single responsible corporate officer misdemeanor and each was sentenced to nine months in prison").

91. *Id.* ("Prosecutors argued that the four acted knowingly, especially after a Synthes medical consultant warned that the tests amounted to 'human experimentation.'").

92. *See* Ivanov, *supra* note 26, at 799–800 (citing United States v. Huggins, Crim. No. 09-403-3, 2011 WL 6180623 (E.D. Pa. Dec. 13, 2011)).

93. *Id.* at 800 ("Based on the evidence accumulated against Huggins during his time at Synthes, it is possible that he would have been convicted of fraudulent misbranding had his case gone to trial.").

94. United States v. DeCoster, 828 F.3d 626, 634 (8th Cir. 2016) ("The dissent [in *Park*] argues that we must treat the FDCA, 21 U.S.C. §§ 331(a), 333(a)(1), as requiring a defendant to know he violated the statute in order to be subject to its penalties because the statute has 'no express congressional statement' to omit a mens rea

Austin "Jack" DeCoster and his son Peter were corporate officers at Quality Egg, a large farm that produced, cleaned, packed, and shipped eggs.[95] The government brought suit when Quality Egg introduced eggs contaminated with salmonella into interstate commerce.[96] The defendants argued that they lacked "actual knowledge" of the contaminated eggs being sold.[97] They were, however, held liable under the Doctrine.[98]

In *DeCoster*, the Eighth Circuit U.S. Court of Appeals discussed the omission of a mens rea requirement, explaining that Congress has not required awareness of wrongdoing in order to hold corporate officers liable for violations under certain statutes protecting public welfare.[99] The DeCosters petitioned the U.S. Supreme Court for a writ of certiorari.[100] In their petition, the defendants argued that the Eighth Circuit's decision in their case "gravely expands" the reach of the Doctrine.[101] However, the Court denied the DeCosters' petition—a decision that, according to some, "assures a continued lack of clarity" regarding the Doctrine's use.[102]

3. The Doctrine Currently

The Doctrine remains in force.[103] The Department of Justice relies on the Doctrine in its enforcement of health-related laws, as the Department of Health and Human Services Office of Inspector General (OIG) initially used the Doctrine to handle fraud in the healthcare industry.[104]

---

requirement. We rely however 'on the nature of the statute and the particular character of the items regulated to determine whether congressional silence concerning the mental element of the offense should be interpreted as dispensing with conventional mens rea requirements.'") (quoting Staples v. United States, 511 U.S. 600, 607 (1994); *see also DeCoster v. United States*, SCOTUSBLOG, http://www.scotusblog.com/case-files/cases/decoster-v-united-states/ [https://perma.cc/F7YN-ZHU9] (last visited Feb. 7, 2020).

95. McGovern et al., *supra* note 63 ("Austin 'Jack' DeCoster owned Quality Egg, and his son Peter DeCoster served as its Chief Operating Officer. Quality Egg operated six farms with 73 barns that had five million hens. They also owned 24 other barns with young chickens, and processing plants for cleaning, packing, and shipping the eggs.") (citing *DeCoster*, 828 F.3d at 629).

96. *DeCoster*, 828 F.3d at 629.

97. McGovern et al., *supra* note 63 ("*DeCoster* is notable because the company's owner and chief operating officer argue they should not be sentenced to prison since they did not have 'actual knowledge' that their egg distribution company sold eggs contaminated with salmonella.").

98. *DeCoster*, 828 F.3d at 629.

99. *Id.* at 634 ("The [Federal Food, Drug, and Cosmetic Act] regulates services and products which affect the health and well being of the public . . . Congress has not required 'awareness of some wrongdoing' in order to hold responsible corporate agents accountable for violating the statute."); *see also* 21 U.S.C.S. § 331 (LEXIS 2019) ("The introduction or delivery for introduction into interstate commerce of any food, drug, device, tobacco product, or cosmetic that is adulterated or misbranded.").

100. *See generally* Michael W. Peregrine, *The "Responsible Corporate Officer Doctrine" Survives to Perplex Corporate Boards*, HARV. L. SCH. F. ON CORP. GOVERNANCE (July 5, 2017), https://corpgov.law.harvard.edu/2017/07/05/the-responsible-corporate-officer-doctrine-survives-to-perplex-corporate-boards/ [https://perma.cc/4T25-QXAQ].

101. McGovern et al., *supra* note 63 ("In their Petition for Writ of Certiorari, the DeCosters argue that the Eighth Circuit's holding, affirming the conviction and sentencing of both executives to three months imprisonment, gravely expands the RCO doctrine and an innocent supervisor convicted of vicarious criminal liability should not face imprisonment.").

102. Peregrine, *supra* note 100 ("The Supreme Court's decision not to take up the DeCoster case assures a continued lack of clarity in the application of the Responsible Corporate Officer Doctrine.").

103. *Id.*

104. Kim, *supra* note 5, at 130 (referencing Daniel R. Levinson, Inspector Gen., Dept. of Health & Hum.

In the years following the cases mentioned above—which focus primarily on public health issues—the Doctrine has expanded its reach to other types of public welfare laws. Examples include the Health Insurance Portability and Accountability Act (HIPAA), "health-related laws" under the Food and Drug Administration (FDA),[105] and laws involving the environment and consumer fraud.[106] The OIG has expanded its use of the Doctrine to hold individual corporate officers accountable for healthcare fraud[107] in the pharmaceutical and medical device industries.[108]

C. Defenses to Liability Under the Doctrine

Because the Doctrine does not include a mens rea element, lack of intent or lack of knowledge defenses will not protect defendants against allegations under the Doctrine.[109] Most affirmative defenses are also ineffective.[110]

The defense most likely to be effective against the Doctrine is simply that the prima facie elements for the Doctrine were not satisfied. Per the case facts, a defense could be that the elements had not been met. The defendant had not been in a position of responsibility, that no such nexus existed, and that the defendant did not facilitate the violations.[111]

The "powerless" defense—also called the "objective impossibility" defense—is the

---

Servs., Keynote Address at the Health Care Compliance Ass'n Ann. Compliance Inst. 5 (Apr. 19, 2010), https://oig.hhs.gov/testimony/docs/2010/hccaigkeynotesummary.pdf [https://perma.cc/5HFL-ZEZB]).

105. *Id.* at 131 ("Public welfare laws . . . encompass health-related laws under the Food and Drug Administration ('FDA'), the Health Insurance Portability and Accountability Act ("HIPAA"), and various fraud and abuse laws impacting the health industry consisting, primarily, of the durable equipment, medical devices, pharmaceutical industry, and providers of healthcare.").

106. *See* Wise, *supra* note 23, at 293 ("The major U.S. environmental statutory schemes are public welfare statutes and currently hold certain individuals, such as owners and operators of facilities, personally responsible irrespective of whether those individuals are also corporate officers."); *see also* Clark, *supra* note 27, at 6 ("In the years after *Dotterweich* and *Park*, courts have allowed prosecutors and regulators to expand [the Doctrine] to other 'public welfare' laws—primarily environmental laws, but also securities laws, as well as 'consumer fraud, deceptive mortgage lending practices, antitrust violations, failures in recordkeeping of controlled substances, sales tax violations, liability under the Sarbanes-Oxley Act, and others.'"); COX & HAZEN, *supra* note 2 (stating that the Responsible Corporate Officer Doctrine "has been invoked in tax matters" including: Purcell v. United States, 1 F.3d 932, 936 (9th Cir. 1993); Erwin v. United States, 591 F.3d 313, 325 (4th Cir. 2010); Jefferson v. United States, 546 F.3d 477, 481 (7th Cir. 2008); Ferguson v. United States, 484 F.3d 1068, 1075 (8th Cir. 2007); Greenberg v. United States, 46 F.3d 239, 240 (3d Cir. 1994); Muck v. United States, 3 F.3d 1378, 1381 (10th Cir. 1993); Kinnie v. United States, 994 F.2d 279, 284 (6th Cir. 1993); and, Hochstein v. United States, 900 F.2d 543, 547–48 (2d Cir. 1990)).

107. Kim, *supra* note 5, at 130 (stating "*OIG is focused on holding Responsible Corporate Officials accountable for health care fraud*" (quoting Levinson, *supra* note 104)) (emphasis in original).

108. *Id.* at 139 ("The corporate officers most affected by the RCOD in the healthcare industry have been from pharmaceutical and medical device companies.").

109. *Id.* at 140 ("The challenge in such strict liability criminal cases is that the defendant cannot defend against the criminal allegations brought against him or her under the RCOD by asserting the standard lack of intent or lack of knowledge defenses, in that they are not the elements of the crime.").

110. *Id.* ("None of the 'standard' affirmative defenses are effective in suits brought by the government, in that they simply dilute the strength of a legitimate defense, if there was any in the first place.").

111. *Id.* at 141 ("[T]he defendant may assert, if available under the facts of the case, [(1)] that [the defendant] was *not* in the position of responsibility *at the time* the alleged improper acts occurred; [(2)] that there is no nexus between [the defendant's] position and the violation in question, in that [the defendant] could not have influenced the corporate actions which constituted the violations; and/or [(3)] that whatever actions or inactions [the defendant] chose to undertake they did not facilitate the violations.").

defense that the corporate officer was indeed not in a position to have been able to prevent, or put a stop to, the violation even if the officer had been aware the violation was occurring.[112] Corporate officers may assert they were "'powerless' to prevent or correct the violation."[113] The Supreme Court in *Park* recognized that even while Congress intended for the Federal Food and Drugs Act to impose "the highest standard of foresight and vigilance" on corporate officers, officers are not expected to do things that are considered "objectively impossible."[114] This defense allows corporate officers to escape unscathed in the event of an entirely unforeseeable accident.[115]

To be considered "objectively impossible," an officer needs to show that even someone "exercising the *Park* standard of the highest 'foresight and vigilance' would have been unable to predict and prevent the outcome."[116] The success of the powerlessness defense ultimately rests on whether the fact-finder believes the corporate officer was powerless,[117] regardless of the actions taken by the corporate officer.

Although a corporate officer may invoke powerlessness to prevent the criminal act as a defense, this defense is very unlikely to succeed.[118]

III. ANALYSIS

To analyze the possibility that the Doctrine could apply to cyber breaches, this Part will evaluate healthcare data breaches and how the Doctrine may apply to those breaches under HIPAA as a "public welfare" statute. It will then evaluate the penalties of liability under the Doctrine in healthcare settings. This Note will then consider ways in which the Doctrine would not apply to cyber breaches, focusing on a balance of powerlessness and control.

A. Healthcare Data Breaches

Healthcare data—"[i]nformation related to health conditions, reproductive outcomes, causes of death, and quality of life"[119]—is helpful in several ways.[120] The data is an

112. United States v. Wiesenfeld Warehouse Co., 376 U.S. 86, 91 (1964).

113. *Id.*; *see also* Kim, *supra* note 5, at 141 (referencing the "powerless" defense in *Park*).

114. United States v. Park, 421 U.S. 658, 673 (1975) ("The duty imposed by Congress on responsible corporate agents is, we emphasize, one that requires the highest standard of foresight and vigilance, but the Act, in its criminal aspect, does not require that which is objectively impossible.").

115. Baird, *supra* note 12, at 961 (explaining that "if the actions that could have prevented the misconduct were impossible, then not having taken those actions is an affirmative defense").

116. *Id.* at 962–63 ("The secretary-treasurer first attempted to argue that it would have been 'objectively impossible' for him to foresee such a chain of events, but the appellate court agreed with the district court that someone exercising the *Park* standard of the highest 'foresight and vigilance' would have been able to predict and prevent this outcome.") (referencing United States v. Y. Hata & Co., 535 F.2d 508 (9th Cir. 1976)).

117. Baird, *supra* note 12, at 978 (explaining that "the success of the defense ultimately rests on the fact finder's individualized sense of what constitutes a sufficient effort").

118. Amiad Kushner, *Applying the Responsible Corporate Officer Doctrine Outside the Public Welfare Context*, 93 J. CRIM. L. & CRIMINOLOGY 681, 700 (2003) ("The impossibility defense has never been successfully raised.").

119. *Health Data*, MCGRAW-HILL CONCISE DICTIONARY OF MODERN MEDICINE (2002), https://medical-dictionary.thefreedictionary.com/health+data [https://perma.cc/RZ28-94F7].

120. *See* Mona Lebied, *12 Examples of Big Data Analytics in Healthcare that Can Save People*, DATAPINE (July 18, 2018), https://www.datapine.com/blog/big-data-examples-in-healthcare/ [https://perma.cc/4WX4-DJLJ] (discussing how collecting and analyzing healthcare data can help more effectively and efficiently treat

essential part of fraud prevention,[121] and enables healthcare organizations to increase efficiency by reducing waste.[122] Patterns found by comparing transaction data with claims and billing records reveal billing discrepancies.[123] Centers for Medicare and Medicaid Services have been able to recover over four billion dollars annually by using data to reduce fraud.[124] Collecting vast amounts of data, however, comes with its own risks as well.

The Doctrine, which applies to "public welfare" statute violations,[125] could apply to cyber breaches—particularly those within healthcare settings, because those breaches can violate HIPAA.[126] Public welfare laws are not necessarily limited to FDC Act provisions but also include Health Insurance Portability and Accountability Act (HIPAA) "and various fraud and abuse laws."[127] One example of a data breach resulting in a HIPAA violation involved three separate breaches and resulted in $5.5 million in fines.[128] Another example involved a large university medical center's loss of an unencrypted flash drive that held information protected by HIPAA.[129] It is important to note that the healthcare companies in both of these examples were determined to have failed to conduct an adequate risk analysis prior to their breaches.[130]

The Department of Health and Human Services (HHS) implemented the Health Information Technology for Economic and Clinical Health (HITECH) Act in 2009, giving HHS the authority to promote the "quality, safety, and efficiency" of healthcare in the information technology context.[131] Under the HIPAA Breach Notification Rule, HIPAA-

---

patients).

121. "Healthcare organizations can reduce improper billing and avoid erroneous or fraudulent claims on a pre-adjudication basis, not risking reputation and financials." Lola Koktysh, *The State of the Art in Health Data Analytics*, SCIENCESOFT (May 16, 2017), https://www.scnsoft.com/blog/health-data-analytics-overview [https://perma.cc/L4KF-7XY7].

122. *Id.* ("[T]he transaction data with claims and billing records is analyzed to find patterns indicating fraudulent activity or other irregularities, resulting in waste and abuse.").

123. *Id.*

124. INST. FOR HEALTH TECH. TRANSFORMATION, TRANSFORMING HEALTH CARE THROUGH BIG DATA 7 (2013) ("In fiscal year 2011, for the second year in a row, CMS anti-fraud activities resulted in more than $4 billion in recoveries, an all-time high, owing in large part to big data-based detection and analytics tools.").

125. COX & HAZEN, *supra* note 2.

126. Lax data security and breaches of protected health information have been known to violate HIPAA. Kim, *supra* note 5, at 139 (referencing Jeff Overley, *Ill. Hospital Chain Inks Record $5.5M HIPAA Deal*, LAW360 (Aug. 4, 2016, 2:57 PM), https://www.law360.com/articles/825148/ill-hospital-chain-inks-record-5-5m-hipaa-deal [https://perma.cc/C5L5-PSTV]) ("Illinois' largest hospital chain will pay $5.5 million for lax data security and breaches of protected health information for millions of patients, a record payout under the Health Insurance Portability and Accountability Act."); *see also The Most Common HIPAA Violations You Should Be Aware Of*, HIPAA J. (Apr. 26, 2019), https://www.hipaajournal.com/common-hipaa-violations/ [https://perma.cc/J4RQ-WT89] [hereinafter *Common HIPAA Violations*].

127. Kim, *supra* note 5, at 131.

128. Ajmal Kohgadai, *HIPAA Violations Examples and Cases – 8 Cautionary Tales*, SKYHIGH NETWORKS, https://www.skyhighnetworks.com/cloud-security-blog/hipaa-violations-examples-and-cases-8-cautionary-tales/ [https://perma.cc/B3G3-VJVY] (last visited Jan. 20, 2020).

129. *See generally* Heather Landi, *New York Health System to Pay $3M HIPAA Settlement*, FIERCE HEALTHCARE (Nov. 6, 2019, 9:20 AM), https://www.fiercehealthcare.com/tech/new-york-health-system-to-pay-3m-hipaa-settlement-for-lapse-security-measures [https://perma.cc/77AA-4WKN].

130. *Id.*; *see also Common HIPAA Violations*, *supra* note 126; Kohgadai, *supra* note 128.

131. *Health IT Legislation*, HEALTH IT (Aug. 28, 2019), https://www.healthit.gov/topic/laws-regulation-and-policy/health-it-legislation [https://perma.cc/R8Z4-SKWS] (stating the HITECH Act of 2009 "provides [the Department of Health and Human Services] with the authority to establish programs to improve health care quality, safety, and efficiency through the promotion of health IT, including electronic health records and private

covered entities must notify the HHS Secretary when a security breach occurs.[132] The HHS has traditionally placed emphasis on cyber breaches affecting more than five hundred individuals.[133] In August of 2016, however, the HHS's Office for Civil Rights issued an alert claiming it would be investigating more health data breaches affecting less than five hundred individuals as well.[134] This could indicate that the HHS is beginning to focus more on cyber breaches, and the Doctrine could conceivably be invoked for cyber breaches in the near future.[135]

A growing body of evidence suggests *Park* prosecutions are going to increase.[136] Among this evidence is the set of criteria the FDA released in February 2011, called "Special Procedures and Considerations for *Park* Doctrine Prosecutions," which provides factors to consider when deciding whether to bring a misdemeanor charge against a corporate officer.[137] While establishing these criteria does not explicitly mean that *Park* prosecutions are going to increase, some scholars believe that the FDA's creation of the guidelines indicates that prosecutions under *Park* are going to become more common.[138]

With the increasing pervasiveness of cyber breaches comes the need to establish who is responsible for the breaches. Usage of the Doctrine could impact liability analysis.[139] While the Doctrine generally is used to enforce FDCA provisions,[140] nothing prevents the application of the Doctrine to other areas of the law.[141] Some scholars believe it is "highly

---

and secure electronic health information exchange").

132. *Breach Notification Rule*, HHS (July 26, 2013), https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html [https://perma.cc/VA45-ZJH2] ("The HIPAA Breach Notification Rule, 45 CFR §§ 164.400-414, requires HIPAA covered entities and their business associates to provide notification following a breach of unsecured protected health information.") [hereinafter *Breach Notification Rule*]; s*ee also* Notification to the Secretary, 45 C.F.R. § 164.408 (2011).

133. *See Breach Notification Rule*, *supra* note 132 (explaining steps that covered entities must take when breaches affect 500 or more individuals).

134. Mary Butler, *OCR to Enforce Investigating Breaches Affecting Under 500 Individuals*, J. AM. HEALTH INFO. MGMT. ASS'N (2016).

135. Kim, *supra* note 5, at 139 (explaining the possibility that the government may begin to pursue corporate officers in the healthcare industry for cyber breaches).

136. Baird, *supra* note 12, at 968 (stating "the mere fact that the criteria have been established and distributed adds to the body of evidence suggesting that Park prosecutions will become more prevalent in the near future").

137. *Id.* at 967–68 (referencing the U.S. FOOD & DRUG ADMIN., REG. PROCS. MANUAL, § 6-5-3, at 54 (2018), https://www.fda.gov/downloads/ICECI/ComplianceManuals/RegulatoryProceduresManual/UCM074317.pdf [https://perma.cc/S75X-WJ4H]) (including factors such as whether the violation involves harm to the public, is obvious, and is widespread, among others).

138. *Id.* at 968.

139. *See generally* Brian Lewis & Steven Woodward, *Corporate Criminal Liability*, 51 AM CRIM. L. REV. 923 (2014).

140. However—while the FDC Act was applied to both *Dotterweich* and *Park*—as previously mentioned in this Note, "the years after Dotterweich and Park" have seen the courts "allow[] prosecutors and regulators to expand [the Doctrine] to other 'public welfare' laws — primarily environmental laws, but also securities laws, as well as 'consumer fraud, deceptive mortgage lending practices, antitrust violations, failures in recordkeeping of controlled substances, sales tax violations, liability under the Sarbanes-Oxley Act, and others.'" Clark, *supra* note 27, at 6 (quoting Martin Petrin, *Circumscribing the "Prosecutor's Ticket to Tag the Elite": A Critique of the Responsible Corporate Officer Doctrine*, 84 TEMP. L. REV. 283, 289–90 (2012)). *See also* Green, *supra* note 73, at 508 ("In the 1990s, the [Responsible Corporate Officer doctrine] was used for civil penalties in cases on a wide range of environmental statutes, including CERCLA, the Clean Air Act, and the Federal Hazardous Substances Act."); *see, e.g.*, Wise, *supra* note 23, at 313.

141. Baird, *supra* note 12, at 951 n.9 ("*Park* doctrine prosecutions have thus far been used almost exclusively to enforce provisions of the Food, Drug, and Cosmetic Act (FDCA) § 1, 21 U.S.C. § 301 (2006), but there is

probable" that the Responsible Corporate Officer Doctrine's reach will grow into other industries, such as finance.[142] Others go even further, stating not only is it "unwise" to focus the Doctrine's application not only on FDCA violations,[143] but also suggesting the Doctrine could, and should, be expanded beyond the public welfare context.

Regardless, some consider cybersecurity a public welfare issue. The National Governors Association "has been focused on engaging states when it comes to cybersecurity," and 39 governors have signed a multistate compact to improve their states' positions in the cybersecurity realm.[144] Some policy analysts state that a cyber-attack could result in "jeopardizing public welfare."[145]

Meanwhile, data breaches are increasing,[146] as are data breach investigations.[147] The continuation of data breaches may shift the government's focus to corporate officers within the healthcare provider industry.[148] In 2016, the HHS's Office for Civil Rights announced they would expand their data breach investigations.[149] The courts view data breaches as harmful to the public welfare, indicating the ubiquity of data breaches does not immunize companies from liability for the breaches.[150]

Finally, in cases that have applied the Doctrine, such as *Dotterweich*, neither the structure of the corporate hierarchy nor the particular industry was a key consideration. Thus, *Dotterweich* and similar cases is persuasive precedent for the proposition that corporate officers in the healthcare industry—or, in the information technology industry—

---

nothing limiting its use only to this particular piece of legislation.").

142. *See* Howard & Woods Anderson, *supra* note 87 (explaining the expectation that the doctrine "will expand to other industries like aviation, construction, and financial services").

143. Kushner, *supra* note 118, at 683 ("The RCO doctrine has been unwisely viewed as a special rule to be applied exclusively to 'public welfare offenses,' such as the food and drug violations implicated in the seminal RCO cases.").

144. Eyragon Eidam, *States Take a Comprehensive Approach to Improving Cybersecurity*, GOV'T TECH. (Aug. 3, 2017), https://www.govtech.com/policy/States-Take-a-Comprehensive-Approach-to-Improving-Cybersecurity.html [https://perma.cc/4YR4-9BXJ]; *see, e.g.*, NAT'L GOVERNORS ASS'N, MEET THE THREAT: A COMPACT TO IMPROVE STATE CYBERSECURITY (2017), https://governor.hawaii.gov/wp-content/uploads/2017/07/1707CybersecurityCompact.pdf [https://perma.cc/8624-TA2D].

145. PATRICIO PORTILLO ET AL., NAT'L GOVERNORS ASS'N, SMART & SAFE: STATE STRATEGIES FOR ENHANCING CYBERSECURITY IN THE ELECTRIC SECTOR 4 (2019), https://www.nga.org/wp-content/uploads/2019/04/NGA-Smart-Safe-State-Strategies-for-Enhancing-Cybersecurity-in-the-Electric-Sector.pdf [https://perma.cc/C5BF-RETA].

146. The number of reported data breaches has been on the rise in the United States since 2011. Juliana De Groot, *The History of Data Breaches*, DATAINSIDER (Oct. 24, 2019), https://digitalguardian.com/blog/history-data-breaches [https://perma.cc/M4RV-EMXM].

147. "The number of data breaches under investigation more than doubled from 2018 to 2019, according to data published by the US Department of Health & Human Services." Ben Heubl, *Analysis: US Healthcare Data-Breach Investigations Skyrocket*, ENGINEERING & TECH. (Dec. 17, 2019), https://eandt.theiet.org/content/articles/2019/12/analysis-us-healthcare-data-breach-investigations-skyrocket/ [https://perma.cc/3QUB-CALL].

148. Kim, *supra* note 5, at 139 ("The government may pursue corporate officers individually within the healthcare provider industry-as they have done in the pharmaceutical industry-if data breaches continue or the government does not think the industry is doing all it can to prevent or minimize those breaches.").

149. *See* Butler, *supra* note 134 (explaining they were expanding their investigation to cover those that affect less than 500 individuals).

150. Kim, *supra* note 5, at 139 ("The Courts have already begun to analogize security breaches with a banana peel argument."); *see, e.g.*, F.T.C. v. Wyndham Worldwide Corp. et al., 799 F.3d 236, 247 (3d Cir. 2015) (viewing each IT breach as a fall on a banana peel, stating "were Wyndham a supermarket, leaving so many banana peels all over the place that 619,000 customers fall hardly suggests it should be immune from liability").

would be held liable under the Doctrine.

B. Penalties of Liability for Health Data Breaches

Penalties have grown increasingly severe for corporate officers found liable under the Doctrine.[151] Legal experts point out that because the penalties have increased since *Park*, the previously applicable Supreme Court precedent no longer applies to the Doctrine.[152] A decade after the Doctrine's origination, the penalty for a violation was usually corrective orders and fines.[153] In the years since the Doctrine was created, case law and use of the Doctrine for newer punishments has led to unpredictable results and severe penalties.[154]

To corporate officers who work in healthcare—where HIPAA and biometrics breaches are most likely—the most "alarming" penalty is the exclusion penalty.[155] The HHS Office of Inspector General started using "exclusions" as a way to deter fraud and abuse within healthcare organizations.[156] The United States Court of Appeals in *Friedman v. Sebelius* held the Department of Health and Human Services could exclude corporate officers from participation in federal health care programs for 12 years following their conviction under the Doctrine.[157]

The two types of exclusions are 1) mandatory exclusions and 2) permissive exclusions.[158] For mandatory exclusions, the Office of Inspector General is required by law to exclude individuals and entities convicted of certain types of criminal offenses from participation in federal health care programs.[159] These mandatory exclusion offenses include, among others, offenses related to state health care programs; patient abuse or neglect; and Medicare or Medicaid fraud.[160] Permissive exclusions are those exclusions the Office of Inspector General may exclude from participation in federal health care

151. *See generally* Howard & Woods Anderson, *supra* note 87.

152. Baird, *supra* note 12, at 954 ("In debating the legality of the government's ability to secure convictions of individuals using the doctrine, the Court was operating in light of then-existing federal penalty and sentencing guidelines, which did not include exclusion. In other words, because the risks involved in the outcome of a Park prosecution are now so much more severe than those that existed under the original sentencing practices, there is no applicable Supreme Court precedent for the current doctrinal use.").

153. *Id.* at 981 ("When the doctrine was originally fashioned in the 1970s and 1980s, the cases against individuals typically resulted in fines, fees, and corrective orders.").

154. *Id.* at 982 (explaining "the threat of multi-year exclusions looms over misdemeanor violations in ways that were not envisioned when the doctrine was originally blessed by the Supreme Court in the mid-1970s").

155. *Id.* at 951–52.

156. Kim, *supra* note 5, at 143 ("The OIG turned to civil remedies of exclusion from receiving reimbursement from federal health programs primarily to address issues of fraud and abuse within large healthcare organizations.") (footnote omitted).

157. Friedman v. Sebelius, 686 F.3d 813, 823 (D.C. Cir. 2012).

158. "Under the authority of the Social Security Act ('SSA'), the Secretary of HHS is responsible for excluding individuals. The SSA sets out the circumstances under which an individual or entity must be excluded (mandatory exclusion) and when an individual may be excluded (permissive exclusion)." Baird, *supra* note 12, at 952 (citing 42 U.S.C. § 1320a-7(c)) (footnote omitted).

159. *Background Information*, U.S. DEP'T OF HEALTH & HUM. SERVS., OFF. OF INSPECTOR GEN., https://oig.hhs.gov/exclusions/background.asp [https://perma.cc/78CC-9P54] (last visited Feb. 28, 2020) [hereinafter *Background Information*].

160. OIG is also required to exclude those convicted of "any other offenses related to the delivery of items or services under Medicare, Medicaid, [or State Children's Health Insurance Program (SCHIP)]" as well as "felony convictions for other health care-related fraud, theft, or other financial misconduct; and felony convictions relating to unlawful manufacture, distribution, prescription, or dispensing of controlled substances." *Id.*

programs based on its discretion.[161] These permissive exclusion offenses include, among others, misdemeanor convictions relating to unlawful dispensing of controlled substances; engaging in unlawful kickback arrangements; and *controlling a sanctioned entity as an owner, officer, or managing employee*.[162]

The medical professional community widely considers exclusions from federal funding to be the most alarming penalty under the Doctrine.[163] The HHS Office of Inspector General has the authority to exclude individuals and entities from receiving reimbursement from federal health care programs.[164] The HHS Office of Inspector General states that "[a]nyone who hires an individual or entity on the [List of Excluded Individuals/Entities] may be subject to civil monetary penalties (CMP)."[165] Exclusion results in what is "effectively an exile from the health care industry since excluded individuals may not work for, or with, any company that receives federal health care funding."[166]

A corporate officer excluded from federal health care funding may not work with any entity that receives federal health funding.[167] This can have widespread implications.[168] An excluded corporate officer will no longer receive federal health care program payments.[169] Not only can an excluded corporate officer not remain in his or her role as a corporate officer,[170] the officer still will not receive funds even if the officer moves to an entirely different profession within the healthcare industry.[171] It is likely that an excluded officer would need to move to a field "wholly unrelated to Federal health care

161. *Id.*

162. *Id.*

163. Baird, *supra* note 12, at 986 ("Perhaps most alarming is the district court's wielding of the exclusion authority while demonstrating a lack of understanding about the U.S. health care industry.").

164. *Id.* at 954 ("[T]he main legal reason this new formulation of the *Park* doctrine should raise concern is that HHS did not possess the authority to exclude individuals from the health care industry until 1977."). *See also Background Information*, *supra* note 159.

165. *Background Information*, *supra* note 159.

166. Baird, *supra* note 12, at 969.

167. *Id.* at 952 ("The federal health care exclusion authority effectively functions to prevent a convicted individual from working for or with any entity that receives funding from a federal health program for a period of years.").

168. *Id.* at 954 (explaining that the unexpected removal of an executive from a public corporation "harms not only the executive himself, but also the corporation's management structure and, ultimately, the shareholders").

169. *Id.* at 968–69 ("In essence, an exclusion is the separation of an individual or corporation from federal health care operations, meaning that an excluded entity is prohibited from receiving any payments from any federal health care program (Medicare, Medicaid, etc.) for a specified term. Additionally, no payment may be made to any entity employing or contracting with an excluded individual or company."); *see also Background Information*, *supra* note 159 ("The primary effect is that no payment will be made for any items or services furnished, ordered, or prescribed by an excluded individual or entity. This includes Medicare, Medicaid, and all other Federal plans and programs that provide health benefits funded directly or indirectly by the United States (other than the Federal Employees Health Benefits Plan).").

170. U.S. DEP'T OF HEALTH & HUM. SERVS., OFF. OF INSPECTOR GEN., UPDATED SPECIAL ADVISORY BULLETIN ON THE EFFECT OF EXCLUSION FROM PARTICIPATION IN FED. HEALTH CARE PROGRAMS 7 (2013) [hereinafter OIG EXCLUSION BULLETIN] (explaining that "an excluded individual may not serve in an executive or leadership role (e.g., chief executive officer, chief financial officer, general counsel, director of health information management, director of human resources, physician practice office manager, etc.) at a provider that furnishes items or services payable by Federal health care programs").

171. *Id.* at 6.

programs."[172] Penalties are high for an excluded officer who violates the OIG exclusion[173]—but penalties are also high for providers employing or contracting with an excluded officer.[174]

C. Powerlessness and Control

The Doctrine applies to public welfare statutes, and cybersecurity is considered by some to be a public welfare issue. Additionally, cyber breaches are increasing. There is a possibility that the Doctrine could, therefore, apply to a violation of a cyber breach statute.

However, cybersecurity breaches are unlike other types of harms in that they are often carried out by third party conduct.[175] This third-party perpetration versus a company's negligence to prevent a breach deserves special consideration when considering liability of a corporate officer. Therefore, control is a critical aspect in determining liability under the Doctrine.

Cyber breach statutes are increasing and evolving.[176] As of January 10, 2019, there is no "overarching federal cybersecurity law," however, certain cybersecurity-related regulations apply to some organizations.[177] Some industries—including the health care sector—have federal regulations that provide stipulations for the management of patient data.[178] As a result, most companies in highly regulated industries with data laws use third

172. *Id.* at 7 ("[A]n excluded individual may not provide other types of administrative and management services, such as health information technology services and support, strategic planning, billing and accounting, staff training, and human resources, unless wholly unrelated to Federal health care programs.").

173. "An excluded person violates the exclusion if the person furnishes to Federal health care program beneficiaries items or services for which Federal health care program payment is sought. An excluded person that submits a claim for payment to a Federal health care program, or causes such a claim to be submitted, may be subject to a CMP of $10,000 for each claimed item or service furnished during the period that the person was excluded. The person may also be subject to an assessment of up to three times the amount claimed for each item or service. In addition, violation of an exclusion is grounds for OIG to deny reinstatement to Federal health care programs." *Id.* at 8–9.

174. *See* OIG EXCLUSION BULLETIN, *supra* note 170, at 11 ("If a health care provider arranges or contracts (by employment or otherwise) with a person that the provider knows or should know is excluded by OIG, the provider may be subject to [Civil Monetary Penalties (CMP)] liability if the excluded person provides services payable, directly or indirectly, by a Federal health care program. OIG may impose CMPs of up to $10,000 for each item or service furnished by the excluded person for which Federal program payment is sought, as well as an assessment of up to three times the amount claimed, and program exclusion.").

175. Most cybersecurity breaches are caused by "third party access." Michael Volkov, *Managing Third-Party Vendor Cybersecurity Risks (Part II of III)*, JD SUPRA (Sept. 11, 2019), https://www.jdsupra.com/legalnews/managing-third-party-vendor-99769/ [https://perma.cc/PH5Y-LWV2].

176. *2019 Security Breach Legislation*, NAT'L CONF. ST. LEGISLATURES (Dec. 31, 2019), https://www.ncsl.org/research/telecommunications-and-information-technology/2019-security-breach-legislation.aspx [https://perma.cc/RCN9-HQG8] ("[L]awmakers continue to add to or change laws related to data breaches. At least 21 states in 2019 considered measures that would amend existing security breach laws.").

177. Kayla Matthews, *Getting Familiar with Cybersecurity Laws: Four Regulations You Should Know*, GLOBALSIGN BLOG (Jan. 10, 2019), https://www.globalsign.com/en/blog/four-cybersecurity-regulations-you-should-know/ [https://perma.cc/M235-G5K4] ("It may be surprising that an overarching federal cybersecurity law doesn't yet exist in the United States. However, that doesn't mean all businesses don't need to comply with cybersecurity standards. That's because some kinds of establishments that offer specific services have applicable regulations.").

178. "Health care is one sector governed by federal regulations for managing patient data." *Id.*; *see also*, *Protecting the Privacy and Security of Your Health Information*, HEALTH IT (Dec. 17, 2018), https://www.healthit.gov/topic/protecting-your-privacy-security [https://perma.cc/6D3W-5X78].

party products to manage their data. In the instance of a security breach, it would make little sense to assign liability to corporations that do not manage their data. Neither these corporations, nor the corporate officers at these organizations, have the knowledge or ability to defend against all data security breaches. Further, "[i]f the government cannot prove beyond a reasonable doubt corporate wrongdoing, it should not be permitted to invoke RCOD as against corporate individuals."[179]

Given the history and purpose of the Doctrine, the Doctrine may extend to corporations that create and manage their data environment and have full control over the architecture. Specifically, the Doctrine is likely to apply to corporations that manage their own data in an environment that uses healthcare data. However, it is important to note that a data breach does not guarantee liability for HIPAA compliance.[180] In fact, according to the American Bar Association (ABA) "[v]irtually all enterprises have been breached and have had at least some of their sensitive information compromised."[181] HIPAA compliance necessitates risk reduction, but the Department of Health and Human Services' Office for Civil Rights does not expect healthcare organizations to cultivate impenetrable cybersecurity defenses.[182]

Control remains important with the addition of the "objective impossibility" defense. Under this defense, most corporate associates "who do everything within their corporate power to ensure compliance with the law, will have a colorable defense" to liability under the Doctrine.[183] A corporation that is using the most current tools available to defend themselves against cyber breaches should not be expected to prevent—or predict—cyber breaches that occur in spite of their best efforts.

Due to the variations in control and applicability of the powerless defense, assessing their liability for security breaches under the Doctrine should hinge upon one distinguishing element: the corporation's ability to influence outside security breaches. If a company uses the most current security and their patient database is still hacked, it was objectively impossible for the company to prevent the breach. If the company left the database sitting on an unsecured server, it was not impossible for the breach to have been prevented. The line should be somewhere in between.

D. Determining Liability

Courts hold individual corporate officers liable separately from holding the

---

179. Kim, *supra* note 5, at 139.

180. *See Common HIPAA Violations*, *supra* note 126 ("Even with multi-layered cybersecurity defenses, data breaches are still likely to occur from time to time[,]" but that the Department of Health and Human Services' Office for Civil Rights (OCR) "understands that healthcare organizations are being targeted by cybercriminals and that it is not possible to implement impregnable security defenses.").

181. Roland Trope & Tom Smedinghoff, *The Importance of Cybersecurity Due Diligence in M&A Transactions*, A.B.A. (Sept. 28, 2017), https://www.americanbar.org/groups/business_law/publications/blt/2017/09/04_trope/ [https://perma.cc/DVF2-NAQV].

182. *See Common HIPAA Violations*, *supra* note 126 ("Being HIPAA compliant is not about making sure that data breaches never happen[,]" but rather, "is about reducing risk to an appropriate and acceptable level. Just because an organization experiences a data breach, it does not mean the breach was the result of a HIPAA violation.").

183. Cogswell, *supra* note 37, at 365 n.128 ("[T]he duty imposed on responsible corporate agents is . . . one that requires the highest standard of foresight and vigilance, but . . . does not require that which is objectively impossible." (referencing United States v. Park 421 U.S. 658, 673 (1975))).

corporation liable. The *Dotterweich* Court explained that corporations can only "act" through the dealings of individuals.[184] Courts can also find corporate officers liable regardless of whether they find the corporate officers' company liable. In *Park*, the company pled guilty, and the president of the company pled not guilty.[185] The question that follows is whether individual officers can be held liable—civilly or criminally—under the Doctrine for a data security breach.

As mentioned above, the elements courts use to determine whether someone violates the Doctrine are: (1) the individual has an influence on corporate policies or activities; (2) there is a nexus between the individual's position and the violation; and (3) the individual's actions or inactions facilitate the violations.[186]

The first element requires that the individual has an influence on corporate policies or activities.[187] In a situation in which a health care information breach occurs, a person in a position of authority would be a person who is responsible for the corporation at which the breach occurs.[188] This would include corporate officers—such as a CEO or president—of a healthcare facility where an information breach occurs.[189]

The second element requires that there is a nexus between the individual's position and the violation. As a person in a position of responsibility at a health care facility, a corporate officer's health care facility imputes on the officer a duty to respond to occurrences with "foresight and vigilance."[190] If a corporate officer of a health care facility had, or should have had, notice of a personal health information breach, there would be a nexus between the position (the corporate officer) and the violation (the cyber breach).

A key consideration in such a situation would be a cyber breach from outside the organization. Cyber breaches that occur from outside of a corporation and are defended with software and cybersecurity experts is different from having the ability to influence the outside security breach. If the corporation creates the online environment, the corporation arguably has control.

The third element requires that the corporate officer's actions or inactions actually facilitate the violation. If there are actions the corporate officer of a health care facility could have taken—but failed to take—concerning a health data breach, then the corporate officer could be liable under this element, even if the cyber breach was not immediately foreseeable. However, the "foreseeable risk of a data breach" is one reason that on January

184. United States v. Dotterweich, 320 U.S. 277, 281 (1943) (holding "the only way in which a corporation can act is through the individuals who act on its behalf").

185. "[A company] and [its president] were charged with violating s 301(k) of the Federal Food, drug, and Cosmetic Act (Act) . . . [the company], but not respondent, pleaded guilty." *Park*, 421 U.S. at 658.

186. "An individual may be found personally liable under [the Doctrine] under the following circumstances: (1) the individual must be in a position of responsibility which allows the person to influence corporate policies or activities; (2) there must be a nexus between the individual's position and the violation in question such that the individual could have influenced the corporate actions which constituted the violations; and (3) the individual's actions or inactions facilitated the violations." FLETCHER CYCLOPEDIA, *supra* note 7.

187. *Id.*

188. Hospital governance structures are widely variable, and "each type of governance structure has different regulatory requirements, accountability and responsibilities." However, corporate officers are persons elected or appointed by the board of directors to manage the daily operations of the hospital. Further, regardless of variation, hospital governance structures "share the same fiduciary duties." Nick Price, *Fundamentals of Hospital Board Governance*, BOARDEFFECT (Aug. 16, 2017), https://www.boardeffect.com/blog/fundamentals-hospital-board-governance/ [https://perma.cc/96G2-6Q83].

189. *Id.*

190. United States v. Starr, 535 F.2d 512, 515 (9th Cir. 1976).

28, 2019, the U.S. District Court for the Northern District of Georgia found that Equifax owed consumers "an independent legal duty of care . . . to safeguard personal information."[191] If all cyber breaches are not foreseeable now, they likely will be soon.

IV. RECOMMENDATIONS

As shown in prior sections, the Doctrine applies to public welfare statutes, and many believe cybersecurity is a public welfare issue. The Doctrine could apply to a violation of a cyber breach statute. If this should occur, legislative recommendations include penalty changes or negating the Doctrine altogether for cyber breaches.

Regardless of whether the Doctrine applies to cyber breaches, breaches are increasing. Corporate officers should institute safeguards to help them remain vigilant when securing their company's data. Corporate options that can help corporate officers include corporate education and the implementation of a corporate compliance program.

A. Legislative Recommendations

Individual officer liability,[192] in conjunction with the lack of consideration of mens rea under the Doctrine, makes the possibility of liability high for corporate officers. With the possibility of an exclusion penalty and based on the FDA's issuance of *Park*-style prosecution guidelines, healthcare data breaches—really, all cyber breaches—could become a problem for corporate officers.

Some scholars suggest the Doctrine should only be invoked if some corporate wrongdoing can be proven beyond a reasonable doubt.[193] At a minimum, it is crucial to balance liability for cyber breaches with rational penalties. One recommendation is to hold the corporate officer liable for data breaches occurring while an agent—a person with an understanding of information technology, who manages data security at the organization—acts on behalf of the corporate officer. Another possibility would be to switch from a strict vicarious liability standard to a negligence standard for cases involving cyber breaches. In the absence of either of the earlier two recommendations, a change in penalty would be reasonable.

1. Strict Liability and Mens Rea

Statutes with a mens rea element have held responsible corporate officers criminally liable for conduct of which the officers actually had no knowledge.[194] In such situations, the corporate officer's knowledge is implied by the officer's position within the company.[195] Just being a corporate officer alone is enough, in some situations, to satisfy

191. Avi Gesser & David Robles, *The Rise of Cyber Negligence Claims: Plaintiffs Find Receptive Judges by Going Back to Basics*, COMPLIANCE & ENFORCEMENT (Mar. 6, 2019), https://wp.nyu.edu/compliance_enforcement/2019/03/06/the-rise-of-cyber-negligence-claims-plaintiffs-find-receptive-judges-by-going-back-to-basics/ [https://perma.cc/M6HT-GUMP].

192. Established by the prima facie elements of the Doctrine in Part II.A of this Note.

193. Kim, *supra* note 5, at 139 ("If the government cannot prove beyond a reasonable doubt corporate wrongdoing, it should not be permitted to invoke RCOD as against corporate individuals.").

194. ELLEN S. PODGOR & JEROLD H. ISRAEL, WHITE COLLAR CRIME 47 (West Academic Publishing, 2 ed. 2018).

195. *Id.* at 48 (discussing United States v. Iverson, 162 F.3d 1015 (9th Cir. 1998)).

the corporate officer's element of knowledge.[196]

Because the indicted corporate officer's level of knowledge is irrelevant for a strict liability offense, the Doctrine's status as a strict liability statute remains a controversial subject of legal debate.[197] Liability is based on whether a corporate officer "had, by reason of his position in the corporation, responsibility and authority either to prevent in the first instance, or promptly to correct, the violation complained of, and that he failed to do so."[198]

In a data breach situation, it could be possible for a jury to conclude a corporate officer is a member of the class of employees with a "responsible relation"[199] to the breach, and that by virtue of the corporate officer's position, the corporate officer had the authority and responsibility to deal with the situation.[200] In the same situation, it may be challenging for a corporate officer to defend themselves by showing they were unable to prevent or correct the violation[201] because the outcome of the impossibility defense "ultimately rests on the fact finder's individualized sense of what constitutes a sufficient effort."[202] A fact finder might find it challenging to determine what "sufficient effort" to prevent a cyber breach would look like.

2. Change from Strict Liability to Negligence Standard

Another option would be for courts to consider negating the Doctrine altogether by changing from strict liability to a negligence standard for corporate officers whose company experiences a cyber breach. In most situations, a company that experiences a cyber breach would experience the cyber breach because of the company's negligence, rather than because of a criminal act committed by or within the company.

3. Penalty Changes

In the absence of either an agency relationship or a change from strict vicarious liability to a negligence standard, it might be prudent to change the penalty. When the Doctrine originally came together 50 years ago, the penalties for violations were typically small fines or fees.[203] Currently, in addition to the much higher, potentially crippling monetary penalties, the added possibility of exclusion from the entire industry[204] or jail

196. *Id.* at 46–47 (discussing United States v. Park, 421 U.S. 658 (1975)).

197. *Id.* at 45.

198. *Park*, 421 U.S. at 673–74.

199. United States v. Dotterweich, 320 U.S. 277, 285 (1943) (opining that the class of persons who stand in "responsible relation" to a violation would "be too treacherous to define or even indicate by way of illustration").

200. *Park*, 421 U.S. at 659 (explaining that, in Park, "[t]he charge adequately focused on the issue of respondent's authority respecting the conditions that formed the basis of the alleged violations, fairly advising the jury that to find guilt it must find that respondent 'had a responsible relation to the situation'; that the 'situation' was the condition of the warehouse; and that by virtue of his position he had 'authority and responsibility' to deal therewith").

201. *Park*, 421 U.S. at 673–74 ("The theory upon which responsible corporate agents are held criminally accountable for 'causing' violations of the Act permits a claim that a defendant was 'powerless' to prevent or correct the violation to 'be raised defensively at a trial on the merits.'" (referencing United States v. Wiesenfeld, 376 U.S. 86, 91 (1964))).

202. Baird, *supra* note 12, at 978.

203. *Id.* at 981 ("The defendant in Dotterweich received a penalty of $500 and probation for a period of sixty days.").

204. *Id.* at 982 ("The fact that a penalty of such disruption is available in connection with strict liability is difficult to resolve with traditional views of strict criminal liability.").

time makes the penalties irrational for a vicarious liability crime. If a corporate officer is to be held liable under strict vicarious liability for an action or inaction of which he/she had no knowledge, the fines should be lessened to an amount consistent with other strict liability crimes and should not include funding penalties that work in effect to exclude the corporate officer from their industry.

B. Corporate Recommendations

Corporate officers are entangled with their corporations. One reason is the Department of Justice's decision to punish people, and not the organizations who operate through those people, to keep an organization "where it should be."[205] For this reason, it is imperative to educate corporate officers on the extent of the Doctrine and to help them understand what they should do to keep their corporation operating in such a way that it does not become liable under the Doctrine. An attentive and responsive corporate compliance program is the best way to prevent liability under the Doctrine as it stands.

1. Education Plan

Not all corporate officers are well-versed in the nuances of corporate law.[206] The corporate officers who do have a solid understanding of corporate law may still struggle to understand the Doctrine. Troublingly, corporate officers often have direct access to the precise data hackers are attempting to find.[207] This makes corporate officers a target—so it is important that they understand how to avoid breaches on their own, even if they rely on a third party to protect their data.[208]

Corporate officers should educate themselves on the reaches of the Doctrine but should also focus on the trends. While healthcare and pharmaceutical industries have been affected so far, nothing is preventing the application of the Doctrine to other legislation, and the Office of Inspector General foreshadowed an investigation into data breaches.[209]

When it comes to cybersecurity, corporate officers need to be involved in understanding the risks.[210] The risks can be understood by engaging in education.[211] In a

---

205. Kim, *supra* note 5, at 146 ("[S]ince organizations operate through people, it is people that should be punished, and not the organizations themselves. In theory, by holding individual corporate officers responsible and excluding the 'bad' individuals, the government will return the organization to where it should be.").

206. Hanna Hasl-Kelchner, *The Law-Abiding Executive*, BIZED (Nov. 1, 2006), https://bized.aacsb.edu/articles/2006/november/the-law-abiding-executive [https://perma.cc/NH5R-MQ6Q].

207. "The responsibility for an organisation's cyber security often falls on the IT department, which historically dealt with the security of IT systems." Matt Johnson, *Who's Responsible for Your Cyber-Security?*, INFOSEC ISLAND (Feb. 12, 2019), http://www.infosecisland.com/blogview/25169-Whos-Responsible-for-Your-Cyber-Security.html [https://perma.cc/927N-XH2L].

208. *Id.*

209. *See supra* Part III.A (discussing breaches in the healthcare and pharmaceutical industries).

210. Dave Fachetti, *The Board's Role in Cyber Risk Management: Advice from Top Directors*, BITSIGHT (Nov. 12, 2018), https://www.bitsight.com/blog/the-boards-role-in-cyber-risk-management [https://perma.cc/H3A3-M6LJ] ("The shortage of security professionals among Board members emphasizes the need for collective responsibility around cybersecurity and cyber risk.").

211. To have effective conversations about topics like understanding cybersecurity risk, boards must be "digitally savvy." Peter Weill et al., *Companies with a Digitally Savvy Board Perform Better*, 19 MIT CTR. FOR INFO. SYS. RES. 1 (Jan. 2019), https://www.pega.com/system/files/resources/2019-05/mit-cisr-digitally-savvy-board.pdf [https://perma.cc/4GLL-RRRS]. A digitally savvy board is one who has "an understanding, tested by experience, of how digital technologies such as social, mobile, analytics, cloud, and the Internet of Things will

healthcare environment, both corporate officers and employees are likely to benefit from a "clear training plan" regarding cybersecurity risks.[212]

Corporate officers may also consider incorporating "ongoing review" into their education plan. "Ongoing review" refers to a survey in which corporate officers are interviewed by a third-party consultant every few years.[213] The purpose of these interviews is to help corporate leaders determine which changes it needs to make to ensure it remains educated.[214]

Regardless of the methods of education used, it is important to continue education and remain current.[215] Technology changes rapidly.[216]

2. Compliance Program

Corporate compliance measures can help protect both the corporation itself and the individuals within the corporation from liability under the Doctrine.[217] The OIG provides the following seven elements that must be implemented by compliance programs in select healthcare sectors:[218]

1. Written standards of conduct and written policies and procedures regarding compliance
2. Designation of chief compliance officer and corporate compliance committee to operate and monitor compliance
3. Regular effective education and training programs for employees
4. A process to receive complaints anonymously and protect reporters from retaliation
5. A system to respond to violations of compliance policies, statutes and regulations and enforce appropriate disciplinary action

---

impact how companies will succeed in the next decade." *Id.* If corporate leadership is not digitally savvy, it can increase its digital savvy through education in the forms of "self-directed learning" and "board-wide education." *Id.* at 2.

212. *See generally* Nick Price, *Training Hospital Board Members About Cybersecurity Threats*, BOARDEFFECT (Sept. 11, 2017), https://www.boardeffect.com/blog/training-hospital-board-members-cybersecurity-threats/ [https://perma.cc/W7D3-7WVP].

213. Weill et al., *supra* note 211, at 3 ("[O]ne strong practice [is] to conduct an annual survey of directors, with in-depth director interviews conducted by an independent consultant every three years to produce recommendations for change.").

214. *Id.* ("Several chairs referenced the annual survey of directors as a great source of information about changes the [corporate leadership] needs, such as adjustments in expertise or a requirement for director education.").

215. Ron Kral, *Governing Cybersecurity: Cybersecurity Committees on the Rise*, CORP. COMPLIANCE INSIGHTS (June 11, 2018), https://www.corporatecomplianceinsights.com/governing-cybersecurity-cybersecurity-committees-rise/ [https://perma.cc/H4W5-GJ6E] (explaining "the right mix of directors coupled with continuing education is prudent").

216. John Hagel et al., *Work Environment Redesign*, DELOITTE (June 3, 2013), https://www2.deloitte.com/us/en/insights/topics/talent/work-environment-redesign.html [https://perma.cc/HNL9-DSUQ] ("Many training programs become out of date, if not obsolete, by the time they are launched. At the same time, many executives also find themselves unable to fill high-skilled positions, and are perpetually searching for and paying a premium for employees with specific skill sets.").

217. Kim, *supra* note 5, at 156 (indicating that these programs can help corporations remain in compliance with "complex regulations," while also protecting "the individuals inside the corporations" who are "in positions to influence decisions within the health-related organizations").

218. *Id.* at 157; Publication of the OIG Compliance Program Guidance for Hospitals, 63 Fed. Reg. 8987, 8989 (Feb. 23, 1998).

6. Audits to monitor compliance and assist in reducing identified problem areas
7. Investigation and remediation of identified systemic problems

It is important for corporate officers within a company to understand the potential for liability under the Doctrine. To prevent their company from being liable under the Doctrine, corporate officers should educate themselves on the reaches of the Doctrine and trends regarding legislation involving the Doctrine. They should also consider the seven elements of a corporate compliance program offered by the OIG.

V. CONCLUSION

The Doctrine is worrisome for corporate officers because it can apply to civil, administrative, and criminal circumstances. A corporate officer can be held responsible for a misdemeanor or a felony under the Doctrine.[219] While the Doctrine has not been applied to a data security breach so far, it would be possible for the Doctrine to be applied to such a breach. Because cyber breaches could affect public welfare, cyber breaches may fall under the Doctrine. Cyber breaches are the result of negligence, not criminal misconduct.[220] Therefore, a negligence standard should be used for cyber breaches. If a negligence standard cannot be used for cyber breaches, then penalties should no longer include exclusions. In the meantime, two ways corporate officers can try to prevent themselves from being held liable under the Doctrine are to educate themselves and their companies and to create corporate compliance programs to prevent security breaches.

219. Kim*, supra* note 5, at 130 (explaining liability under the Doctrine).

220. Jared Magill, *The Crooked Path to Determining Liability in Data Breach Cases*, WIRED (Mar. 2015), https://www.wired.com/insights/2015/03/crooked-path-determining-liability-data-breach-cases/ [https://perma.cc/A289-5RZP].