INTRODUCTION

Today, over ninety percent of stock trades are done electronically through financial institutions, exchanges, and brokerage houses.¹ Paper transactions—effectuated by the transfer of a physical stock certificate—

¹ Andrea M. Matwyshyn, Corporate Cyborgs & Technology Risks, 11 MINN. J.L. SCI. & TECH. 573, 586 (2010) (“Approximately only three percent of the trading volume on the NYSE is done by means of traditional ‘open outcry’ trading with humans; 97% of NYSE trades are executed using electronic communication networks.”).
are rare and, for that matter, outdated.\textsuperscript{2} And as a result of industry efforts to phase out the stock certificate, many investors today can no longer reify their stock ownership with a paper certificate.\textsuperscript{3} Yet despite attempts to modernize the commercial law governing investment securities to account for these changes through revisions to Article 8 of the Uniform Commercial Code ("U.C.C."),\textsuperscript{4} it is questionable whether those rules of law remain relevant and effective today, particularly in light of the newest challenges to the U.S. securities markets. Specifically, the recent rise in cybercrime, and hacking in particular, poses risks to the securities trading system that were likely unanticipated by the drafters (and revisers) of Article 8. With strong indications that a cyber attack on the U.S. securities markets is imminent, it may be time for the legal and financial communities to consider revising Article 8 once more.

This Article offers a start in that direction by exploring the cybercrime risk, the property ownership questions that might arise from a hack, and the consequences of judicial misapplication or misunderstanding of Article 8. To that end, Part I elaborates on the risk that a major securities platform will be hacked. Part II then provides an overview of how securities are traded today. It also explores the structure of U.C.C. Article 8 and, in particular, how Article 8 is intended to resolve ownership disputes when securities are illegally transferred. Part III considers how courts might apply Article 8 in resolving the ownership questions that would arise from a securities cyber attack. Part IV concludes with a brief examination of how Article 8 might be amended to avoid investor uncertainty and confusion, which could threaten the stability of the U.S. capital markets.

\textsuperscript{2} See Graham Bowley, \textit{The New Speed of Money}, N.Y. TIMES, Jan. 2, 2011, at BU1. (discussing the "new technological order" of trading). As James Steven Rogers notes:

A generation or more ago, the principal mechanism of settlement in the securities markets was physical delivery of certificates representing securities. If one traced the history of securities clearance and settlement back far enough, one would presumably find a period at which each individual trade was settled by a corresponding delivery of a physical certificate, followed, in the case of registered securities, by registration of transfer on the issuer's books. In most markets, that stage was passed long ago . . . .


\textsuperscript{3} See \textit{infra} notes 44–56 and accompanying text.

\textsuperscript{4} See David C. Donald, \textit{The Rise and Effects of the Indirect Holding System} 41 (Sept. 26, 2007) (unpublished manuscript), \textit{available at} http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1017206 (discussing how the 1994 revisions to U.C.C. Article 8 adapted the Code to account for the system of "immobilization" and the development of an "indirect holding system") Both of these concepts are discussed \textit{infra} Part II.
I. ON THE VERGE OF ATTACK?

“Hacking” is one form of “cybercrime;” that is, criminal activity perpetrated over the Internet. There have been many hacking attacks over the past several years. Some have attracted significant media attention and others are less well known. It is beyond peradventure, though, that “hacking” is the crime de jure, and a threat not only to the U.S. financial system but also to national security.

A. The Cybercriminal Trend

There is a long list of banks, companies, and governmental entities that have recently become victims of a hack. With respect to national security, at least some foreign governments have come to view hacks on the U.S. securities markets (or U.S. corporations) as a viable tactic for harming U.S. interests. China, for example, is suspected of having a division of its army dedicated to hacking. Both China and Russia have demonstrated an interest in weakening the U.S. economy more generally, as evidenced by their seemingly strategic sales of U.S. treasury holdings in the aftermath of the 2008 financial crisis.

For further concrete evidence that hacking is en vogue among criminals, one need only consider the events of the past two years. Newsworthy cyber attacks have been waged on major corporations like

---

5. Thomas A. Petee, et al., Defining “Cyber-Crime”: Issues in Determining the Nature and Scope of Computer-Related Offenses, in 5 Future Challenges of Cybercrime 6–7 (Toby Finnie, Tom Petee & John Jarvis eds., 2010), available at http://fwg.cos.ucf.edu/publications/FWGV5Cybercrime.pdf (proceedings of the FBI Futures Working Group); see also PAUL A. TAYLOR, Hackers: Crime in the Digital Sublime, at xi (1999) (“The currently accepted meaning of the word [hacking] relates to the unauthorised access to and subsequent use of other people’s computer systems.”). As this broad definition suggests, a hacker need not necessarily be a person external to the victim-organization, but could also be a person “inside,” who accesses and abuses his employer-organization’s information systems.

6. See infra notes 10–31 and accompanying text.

7. See infra notes 10–31 and accompanying text.


Apple and Google, and on banks such as Morgan Stanley and Citigroup.\(^{10}\) On June 2, 2011, it was reported that a group of Chinese hackers penetrated Google Gmail accounts, targeting U.S. government officials, Chinese political activists, officials in several Asian countries, military personnel, and journalists.\(^{11}\) And that was not the first time that a group of Chinese hackers had penetrated Google’s system. In January 2010, Google was the victim of a cyber attack under the code name “Operation Aurora.”\(^{12}\) That time, the Chinese hackers targeted “at least 34 companies in the technology, financial and defense sectors.”\(^{13}\) The hackers’ objectives ranged from the theft of email passwords or other personal information, to corporation source code or trade secrets.\(^{14}\) Most recently, Chinese hackers successfully hacked into the U.S. Chamber of Commerce, “gain[ing] access to everything stored on its systems.”\(^{15}\) Though it appears that these attacks came from private citizens, some have alleged that the Chinese government either directly or indirectly supported their activities.\(^{16}\) The cyber attack on

---


13. Id.; see also Michael Joseph Gross, *Enter the Cyber-Dragon*, VANITY FAIR, Sept. 2011, at 220, 220 (discussing recent hack attacks that have originated in China).


16. See Gross, supra note 13, at 222 (“In some cases, the evidence suggests that government and military groups are executing the attacks themselves. In others, Chinese authorities are merely turning a blind eye to illegal activities that are good for China’s economy and bad for
Apple came in July 2011 from a group called “AntiSec,” which allegedly extracted private data from the Apple Inc. server. These are not the only examples: Sony, AT&T, the U.S. Senate, and the CIA have also been recent victims of cyber attacks.

The financial sector is equally vulnerable. In 2008, LPL Financial, the largest independent contractor broker-dealer in the industry, was hacked. The attackers obtained clients’ unencrypted names, addresses, and social security numbers, and compromised the passwords of fourteen financial advisers and four assistants. The hackers attempted to place more than $700,000 in securities trades in connection with nineteen different companies.

The Nasdaq Stock Exchange has also been the subject of recent cyber attacks. The Wall Street Journal reported that “[h]ackers have repeatedly penetrated the computer network of the company that runs the Nasdaq Stock Market during the past year.” Investigators have yet to definitively determine the hackers’ motives, but have considered possibilities such as “unlawful financial gain, theft of trade secrets and a national security threat designed to damage the exchange.” The “mystery” regarding the identity and motivation of hackers is worrisome as investigators remain unsure of whether they have remedied the security gaps, potentially leaving the stock exchange exposed to new forms of attack.

Lastly, a security thinktank, Stratfor, was hacked on December 25, 2011, by a hacking movement known as “Anonymous.” The hackers stole credit card numbers and other personal information of Stratfor’s clients.

---

20. Id.
23. Id.
24. Id. The Hong Kong stock exchange was more recently hacked in August 2011, causing some trading to be suspended for a day and a half. Hong Kong Share Trading Hit by Hackers, BBC (Aug. 11, 2011), http://www.bbc.co.uk/news/technology-14489077.
Based on these incidents, it appears not just possible, but probable, that hackers—whether private or foreign government sponsored—will soon focus their efforts on a major U.S. securities exchange or brokerage house.

As mentioned, the vast majority of securities transactions today are executed through electronic networks and channeled through financial institutions.\(^{27}\) For whatever reason, these electronic networks have demonstrated themselves to be vulnerable to cyber attack, and the responsible institutions have been unable or unconcerned with fortifying them against hacks.\(^ {28}\) As evidence of this vulnerability, “source code for at least three proprietary high frequency trading platforms”—including Goldman Sachs, UBS, and Societe General—“has already been stolen by rogue insiders.”\(^{29}\) As Andrea Matwyshyn aptly noted with respect to these and other banks, “[t]here is reason to question whether stringent information security practices are in place with respect to these companies’ proprietary trading platforms.”\(^ {30}\) Consequently, “the information security of the transactions and the management of the machines performing them create potential for serious [securities] market disruption and provide an attractive target for information criminality.”\(^ {31}\)

B. A Lesson To Be Learned from Europe: The Carbon Credit Crisis

The recent carbon credit theft in Europe provides insight into how a cyber attack on U.S. securities markets might unfold. Major power companies and industrial polluters in the European Union (“E.U.”) are required to obtain a carbon dioxide (“CO\(_2\)” ) emissions certificate for every ton of greenhouse gas emitted in their operations.\(^ {32}\) In November of 2010 and January of 2011, hackers attacked the market in these CO\(_2\) emissions

---

\(^{26}\) Id.

\(^{27}\)  See supra note 1 and accompanying text.

\(^{28}\)  See TAYLOR, supra note 5, at 85. As Taylor’s industry research uncovered more generally, at least in the late 1990s, “approaches to computer security were . . . often apathetic. . . . [A]fter a computer security breach has received large coverage in the media, organisations tend to be more concerned about their security, a concern that quickly fades once the short-term memory of the breach has faded.” Id.


\(^{30}\)  Matwyshyn, supra note 1, at 590.

\(^{31}\)  Id. at 587.

certificates, which are also traded electronically.\textsuperscript{33} The thefts began in Romania, and then spread to Austria and the Czech Republic.\textsuperscript{34} E.U. officials did not know how the crime was being perpetrated and, powerless to stop it, halted trading.\textsuperscript{35} As one blogger for the \textit{Wall Street Journal}: Europe described it:

[A] savvy hacker, who has a thorough understanding of how the European Union’s CO\textsubscript{2} emissions allowances are electronically traded, broke through electronic security systems and transferred millions of virtual certificates that have a very real street value to several different locations. Then the perpetrator likely resold the goods for a handsome profit before authorities knew what happened. A few keystrokes and the hacker’s a multi-millionaire.\textsuperscript{36}

The ownership problems that emerged in the aftermath of the carbon credit hack illustrate what could also happen here in the wake of a cyber attack on a U.S. trading platform. After the carbon credit theft, it was difficult to discern the true ownership of the stolen credits because credits do not have individual serial numbers that are checked during electronic transfer, so subsequent purchasers could easily ignore the risk that they were dealing in stolen property.\textsuperscript{37} Furthermore, the movement of the credits is not electronically monitored; therefore, tracing the stolen credits was extraordinarily difficult.\textsuperscript{38} Perhaps most significant was the “psychological impact of the thefts.”\textsuperscript{39} As a result of the thefts, market participants feared “how to recover stolen credits and how to avoid unwittingly buying stolen credits.”\textsuperscript{40}

A hack would likely have similar effects on the U.S. securities market. Like the carbon credit market, individual securities in the United States are not readily identifiable (there are no “serial numbers” for individual shares), and, as a consequence, individual shares cannot be traced through the Internet.\textsuperscript{41} As a baseline, then, it seems relatively clear that confusion over ownership would arise if a brokerage or exchange house was hacked.

\begin{footnotes}
33. Id.
35. Carney, \textit{supra} note 32.
36. Id.
37. Id.
38. Id.
40. Id.
41. \textit{See infra} notes 121–23 and accompanying text (describing the tracing problems inherent in the modern U.S. securities system).
\end{footnotes}
and the securities on its “books” were stolen and transferred. Unclear ownership rights in the securities market are problematic, primarily because uncertainty can slow or halt trading. As was seen in the 2008 Financial Crisis, a drastic reduction in securities transactions due to investor fear and/or market uncertainty “crunches” the credit markets and reduces liquidity.42 At least one lesson from that crisis is that credit and liquidity problems, if not isolated, can “restrain[] economic growth, stir[] recession fears, and aggravate[] global financial turmoil.”43

Arguably, however, any uncertainty and attendant investor anxiety that would arise from a hack-related crisis could be avoided with clear rules of law that protect the ownership rights of investors who acquire securities in the aftermath of a cyber attack—the subsequent investors or purchasers of securities. Providing protection for subsequent purchasers could attenuate concern that trading in a hacked security would ultimately be to the investor’s legal and financial detriment.

The balance of this Article argues that, with sufficient incentive to keep trading, a short-term crisis catalyzed by a hack could be contained without escalating into a full-scale financial crisis. The question remains, however, whether the law would provide such incentive by adequately protecting purchasers in the wake of a cyber attack. Before exploring that problem in Part III, the next Part provides an overview of how securities are owned today.

II. OWNING AND TRADING SECURITIES IN THE INDIRECT HOLDING SYSTEM

As alluded to above, given the extent to which trading is electronic today, securities ownership is largely intangible, shares are held in fungible bulk, and stock certificates have been phased out of circulation.44 This change in securities ownership begs the question: how does a typical investor today “own” securities?

A bit of historical perspective is instructive. The traditional notion of an investment security is equity ownership in a corporation.45 That concept holds firm today, but the method of ownership has changed. For the hundred years prior to the 1970s, owners held securities “directly” and in

44. See infra notes 45–60 and accompanying text.
45. See James Steven Rogers, Negotiability, Property, and Identity, 12 CARDOZO L. REV. 471, 471–78 (1990) (describing the historical development of investment securities, which were generally either interests in an “enterprise” or shares in public debt).
As one scholar described, “[t]he legal regime that reigned since the early twentieth century in the transfer and registration of securities [was] based upon a model involving the reification of the property interest into a physical certificate.” In this ownership model, there was a direct relationship between the issuer (the company in which the investor held stock) and the investor. The shareholder would receive dividends directly from the issuer, and there would be some form of physical delivery of a stock certificate to settle trades. Investors’ securities were registered in their names.

This model changed in the 1960s and 1970s. In response to the “paper-crunch” of the late 1960s, the market (and regulators) recognized the need to move away from papered securities transactions by eliminating the physical delivery of stock certificates to consummate trades. The goal was to eliminate dependency on stock certificates by “dematerializing” all


48. *Id.* at 667–68.


50. Schroeder, *supra* note 46, at 359 (noting that in the direct holding system, the beneficial owner is also the record owner).

51. Hakes, *supra* note 47, at 668. The so-called paper-crunch of 1967–1970 spurred the Securities and Exchange Commission (“SEC”) to take action toward implementing a paperless transfer system. During the paper-crunch, securities brokers were unable to keep up with the increased volume in trading. Because of the backlog, many brokerage firms were unable to deliver securities on the settlement date and, as a consequence, suffered significant financial losses. See Elisabeth Ledrut & Christian Upper, *Changing Post-Trade Arrangements for OTC Derivatives*, BANK FOR INT’L SETTLEMENTS Q. REV., Dec. 2007, at 83, 88 (describing the paper crunch that occurred between 1967 and 1970 and the SEC’s reaction).

investment securities. However, rather than adopt a system of actual dematerialization, whereby issuers would dematerialize share certificates themselves, the transition to a paperless system of trading was accomplished by “feign[ing] dematerialization” through a process known as “immobilization.” For all intents and purposes, immobilization worked just as well because, “[w]ith respect to paperwork, total immobilization has the same effect as dematerializing the entire market.” Though the technicalities of immobilization and dematerialization are beyond the scope of this Article, a brief overview is helpful to illustrate how the ownership rights of the investor have become dependent on the financial intermediary in this system.

The process of immobilizing securities involves registering actual ownership of securities in a central depository system. An issuer-corporation will issue a “jumbo” stock certificate, representing all the securities from a particular issuance, rather than individual certificates to each investor for his shares. A central depository then holds the jumbo certificate and it, in turn, sells securities to financial intermediaries (banks and brokerage houses), who then hold the securities for themselves or for their customers (individual and institutional investors). Claims to those mutual funds and federal government debt securities, as distinct from investment securities, are all issued in uncertificated form. Schroeder, supra note 46, at 322 n.74.

53. See Schroeder, supra note 46, at 310–12.

54. Donald, supra note 4, at 15 (discussing the choice between actual dematerialization or “feigned dematerialization”); Schroeder, supra note 46, at 324. Following the paper-crunch, immobilization was imposed on all exchange-traded securities by law. Donald, supra note 52, at 58 (“As amended, § 17A Exchange Act requires the SEC to ‘use its authority . . . to end the physical movement of securities certificates in connection with the settlement among brokers and dealers of transactions in securities,’ i.e., to impose the immobilization of securities certificates in a depository.” (quoting 15 U.S.C. § 78q-1(e) (2006))). See generally Luc Thévenoz, Intermediated Securities, Legal Risk, and the International Harmonization of Commercial Law, 13 STAN. J.L. BUS. & FIN. 384, 384 (2008) (examining “the international compatibility of national laws regulating the holding and transfer of securities held with an intermediary”).

55. Donald, supra note 4, at 39.

56. Though some investment securities are still held directly, the vast majority are held indirectly, through intermediaries. See Hakes, supra note 47, at 677 n.81 (noting that, at least in 2002, sixty to eighty percent of securities traded over-the-counter or on exchanges are held indirectly thanks to their immobilization); infra note 69. The primary focus of this Article is indirectly held securities and the implications for bona fide purchasers transacting in that context.

57. See Donald, supra note 52, at 60.

58. See Donald, supra note 4, at 15 (noting that immobilization “allow[s] intermediaries to create a kind of feigned dematerialization by locking the material certificates in their vaults and acting as custodians and fiduciaries”). See generally Martin J. Aronstein, Robert Haydock, Jr. & Donald A. Scott, Article 8 Is Ready, 93 HARV. L. REV. 889, 889–91 (1980) (setting “immobilization” in historical context). As the Securities Industry Association explains the concept,
securities are transferred against the depository’s accounts (or “books”), instead of shares themselves. In the United States, the central depository most often used in this process is an organization that is sanctioned by both Congress and the Securities and Exchange Commission (“SEC”), named Cede & Co. Generally speaking, immobilizing stock certificates facilitates rapid, efficient—and electronic—securities transactions.

Because of the way in which immobilized (or, sometimes, dematerialized) securities are technically held by financial intermediaries

[]Immobilization is any circumstance where an investor does not receive a physical certificate upon the purchase of shares or is required to physically deliver a certificate upon the sale of shares. Evidence of an investor’s ownership will be maintained on the books and records of a broker/financial institution or corporate issuer.

SEC. INDUS. ASS’N, supra note 52, at 3. Pursuant to this model, “all outstanding shares . . . [are placed] in one depository and in the name of one person, so that transfers on that person’s books would resemble a complete dematerialization of the market.” Donald, supra note 4, at 17. As noted subsequently, that “person” is most frequently Cede & Co. See infra notes 60–62 and accompanying text.

59. Donald, supra note 52, at 45.
60. Thévenoz, supra note 54, at 400–01. Cede & Co. is the nominee for the Depository Trust Company (“DTC”), the clearing house that holds shares in its name for other financial institutions. Id. at 401. DTC is a subsidiary of the Depository Trust and Clearing Company (“DTCC”), the entity that clears and settles nearly all securities transactions in U.S. markets. Donald, supra note 4, at 24. The DTCC system includes over ninety-nine percent of depository-eligible securities in circulation. Id. at 39.
61. See Rogers, supra note 45, at 471 (noting that the “difficulties now facing the law of securities transfer seem to be associated with the transition from paper to electronic representations of investments” ushering in the “unnerving prospect that possession of paper embodiments of rights will no longer furnish the fundamental benchmark for adjudication of conflicting claims”).
62. Today, equity securities (as opposed to government securities and mutual funds) may be actually dematerialized in connection with the Direct Registration System (“DRS”), a program that was launched in 1996 as an alternative to immobilization and the indirect holding system. See Donald, supra note 4, at 50. Notwithstanding the lack of paper, dematerialized securities may also be centrally registered under the name of Cede & Co. Id. at 51–52. However, the DRS also offers shareholders the option to hold their shares with the issuer’s transfer agent and register their own names (as opposed to that of an intermediary) on the stockholders list. . . . Today, a retail investor will at the time of making a purchase state on her instruction to the broker whether she wishes to hold her shares in DRS in her own name or through her broker in the name of Cede & Co. If the investor indicates no preference, each share . . . will automatically be placed in DRS and registered in the buyer’s name.

Id. Accordingly, dematerialized securities and DRS may, but will not always, implicate the indirect holding system. Therefore, the discussion above assumes that the effects of dematerialization on an investor’s property rights will be identical to those accompanying immobilization only insofar as the investor opts to register his shares through a broker. Importantly, where the investor participating in the DRS system opts to hold his shares in his own
for the benefit of their customers, this system of “holding” (i.e., owning) securities is said to be “indirect.”

Pursuant to U.C.C. Article 8, holding securities indirectly has several important implications for the investor’s ownership rights. First, the central depository is the registered owner of the security and the participants in the depository system (i.e., financial intermediaries, such as banks and brokers) and their customers (i.e., individual and institutional investors) hold security “entitlements.” The investors are, technically speaking, only the beneficial owners of those entitlements. Second, and related, securities held indirectly are in “street name” and in book entry form. This means that “[t]he security is registered in the name of your brokerage firm on the issuer’s books, and . . . you do not receive a certificate. Instead, your broker keeps a record in its books that you own that particular security.” Third, these entitlements are fungible on the books of the intermediary. In other words, an entitlement holder has a right to a particular quantity of securities, but not to any particular securities themselves. The concept is analogous to money in a commercial bank account (save, of course, the customer’s ability to “withdraw” its securities in physical form in the way that one can withdraw cash from a bank).

Because of these characteristics of the indirect holding system, the investor’s property right under Article 8 is derivative of the financial intermediary, which, as will be seen, affects the nature and extent of any ownership claims he might have in the event his security entitlements are stolen. The next Part of this Article returns to the concept of protecting purchasers and considers how Article 8 attempts to do so. It ends with an argument that Article 8’s efforts at purchaser protection would not prove effective in the face of a hack.

name, it is the investor—not the intermediary—who must qualify as a “protected purchaser” in any hack scenario. See discussion infra Part III.

63. Hakes, supra note 47, at 664 n.2.
64. Thévenoz, supra note 54, at 384, 386, 400–01.
65. Id. at 401.
68. See Hakes, supra note 47, at 688, 776; Schroeder, supra note 46, at 326.
69. See Hakes, supra note 47, at 689 (noting that, in the indirect holding system, an entitlement holder is extremely limited in its rights to a financial asset (including, inter alia, the investment security) against anyone other than the financial intermediary); see U.C.C. § 8-102 cmt. 9 (1994).
III. U.C.C. Article 8: The Protected Purchaser

Article 8 of the U.C.C. governs investment securities—investment transfers, the rights and liabilities of investors, and the financial intermediaries who facilitate these transfers. In general, “Article 8 . . . encompasses the property rules for the transfer and registration of interests in securities and rules on how securities are evidenced.” Article 8 was revised significantly in 1994, in large part to address the realities of the indirect holding system that had developed since the late 1960s. With a focus on promoting negotiability and efficient transactions, the drafters of these revisions were specifically concerned with increasing the protections afforded to securities purchasers (investors). Accordingly, the drafters aimed to “make[] more clear the rules protecting all purchasers against adverse claims that, under previous law, applied only to certain categories of transfers.”

But would these purchaser protection rules—implemented over a decade ago—suffice in the wake of a cyber attack? This Part first examines the protections Article 8 affords to purchasers in the indirect holding system. It then considers how courts would likely apply these rules to claims arising from a hack. It concludes with a discussion of the possible

---

70. Technically speaking, the term “protected purchaser” in Article 8 of the U.C.C. applies only to directly held securities, which is governed by section 3. See U.C.C. § 8-303 (1994). As will be discussed, the protections afforded purchasers of indirectly held securities are governed by three distinct provisions in section 5. See id. §§ 8-502, 8-503, 8-510. For ease of reference, the balance of this Article refers to all of these provisions in section 5 as “protected purchaser rules.”

71. The U.C.C. is not a comprehensive codification of securities law. Rather, [t]he UCC governs only certain issues relating to the conveyancing of interests in investment securities, including the creation and perfection of security interests, the mechanics of securities transfers, the priorities of competing claimants of interests and the distribution of assets in the rare cases when broker-dealers have shortfalls of securities which are not administered by federal bankruptcy or receivership proceedings. Schroeder, supra note 46, at 350. It is important to bear in mind that “Article 8 simply encompasses the property rules for the transfer and registration of interests in securities and rules on how securities are evidenced. It does not attempt to regulate the relationship between customer and broker or among brokers and clearing corporations.” Hakes, supra note 47, at 670.

72. Hakes, supra note 47, at 670. One of the goals of Article 8 was to reduce the “legal uncertainties that surrounded the indirect holding system[, which] adversely affected everyone involved in the securities markets.” Id. at 665. The revisions “established a new legal regime to comport with the market realities of transferring and registering securities held indirectly (through a broker or other intermediary).” Id. at 664.

73. See Schroeder, supra note 46, at 351, 357–58.

74. See id. at 351–53; Hakes, supra note 47, at 673–75.

75. Rogers, supra note 2, at 1434. These revisions have been adopted by all fifty states, the District of Columbia, and the U.S. Virgin Islands. Thévenoz, supra note 54, at 395.
A. The Four Layers of Purchaser Protection in Article 8

Under the common law principle of *nemo dat quod non habet*, one cannot acquire title better than that held by the person from whom he acquired property. That principle has been used to support the proposition that one cannot gain good title from a thief. In some contexts, however, the common law provides an exception to *nemo dat* for “bona fide” or “good faith” purchasers who lack notice of any adverse claims to the property. Several Articles of the U.C.C. have incorporated these common law principles, including Article 8. As in many commercial contexts, the drafters of Article 8 recognized that the success of the securities markets turns on negotiability and, accordingly, embraced the bona fide purchaser principle. The drafters understood that protecting (bona fide) purchasers avoids the risk that “settled trades can be upset” by promoting the finality of transactions.

Section 8-502 sets out the generally applicable protected purchaser rule in the indirect holding system. It provides: “An action based on an adverse claim to a financial asset, whether framed in conversion, replevin, constructive trust, equitable lien, or other theory, may not be asserted against a person who acquires a security entitlement . . . for value and without notice of the adverse claim.”

---

76. See J.P. Benjamin, A Treatise on the Law of Sale of Personal Property 7 (Hurd & Houghton eds., 2d ed. 1877); Schroeder, supra note 46, at 296 n.6 (“This is the familiar principal that one has the power to transfer only what one owns.”). The rule of *nemo dat quod non habet* is the term generally used in E. Allan Far实质性 et al., Cases and Materials on Commercial Law (5th ed. 1993).

77. Benjamin, supra note 76, at 11.

78. See U.C.C. § 2-403(1) (2003) (“A person with voidable title has power to transfer a good title to a good-faith purchaser for value.”); U.C.C. § 2-102 cmt. 20 (2011) (electronic pocket part update) (discussing how the concept and definition of “good faith” applies throughout the Code); see also Steven J. Burton, Good Faith in Articles 1 and 2 of the U.C.C.: The Practice View, 35 WM. & MARY L. REV. 1533, 1533 & n.1, 1534 (1994) (discussing the “specific requirements of good faith” within the U.C.C. and providing a list of sections that mention good faith).

79. Hakes, supra note 47, at 674.


81. Id. at § 8-502; see Kenneth C. Kettering, Repledge Deconstructed, 61 U. PITT. L. REV. 45, 111 (noting that section 8-502 “sets forth a modernized version of the traditional bona fide purchaser rule, reshaped to fit the indirect holding system”).

82. U.C.C. § 8-502 (1994). It is important to note, however, that section 5 of Article 8 has three provisions pertaining to purchaser protections, U.C.C. sections 8-502, 8-503(c), and 8-510. See supra note 70 and accompanying text. Section 8-502 deals with adverse claims to a financial
Using this language, the drafters intended to give securities purchasers greater protection than the common law’s bona fide purchaser doctrine. Specifically, as Hakes identifies, section 8-502 created “layers” of protection for investor-purchasers that exceed what the common law ordinarily provides. First, in section 5, revised Article 8 shifted the burden of proof from the purchaser, as part of his defense to an adverse claim (i.e., proving that he is, in fact, a purchaser for value without notice of an adverse claim), to the adverse claimant, as a required element of a prima facie case for an adverse action. Second, the drafters eliminated any mention of “good faith” (the English equivalent of “bona fide”) as a requirement for receiving purchaser protections under Article 8. Third, the revisions rejected the “open-ended concept” of notice, making it harder to establish constructive notice. Fourth, under section 8-502, a purchaser’s protection can be defeated only by showing notice of a specific adverse claim, as opposed to notice of any adverse claim, which is all that the asset asserted against another entitlement holder. Hakes, supra note 47, at 712. Aside from section 8-502, the other two sections are nearly identical in language. Section 8-503 provides: An action based on the entitlement holder’s property interest with respect to a particular financial asset under subsection (a), whether framed in conversion, replevin, constructive trust, equitable lien, or other theory, may not be asserted against any purchaser of a financial asset or interest therein who give value, obtains control, and does not act in collusion with the securities intermediary.

U.C.C. § 8-503(e). One noteworthy difference between section 8-503(e) and section 8-502 is the former’s use of a “no-collusion” rather than a no-notice standard. Hakes, supra note 47, at 720. In practice, however, others have questioned whether there is a meaningful distinction between “collusion” and “notice.” See infra note 97. Section 8-503(e) applies specifically to adverse claims to the financial asset itself and protects secured creditors and “repo” purchasers. Hakes, supra note 47, at 721. Indeed, Hakes argues, section 8-503(e) could probably be said to apply to “most adverse claims that could arise.” Id. at 719.

Section 8-510 differs from section 8-502 only insofar as the purchaser who resorts to section 8-510 must “obtain[] control” of the entitlement or financial asset in order to receive the protection. Id. at 716. As Hakes explains, section 8-510 likely covers secured creditors who have a security interest in the security entitlement, a repo purchaser of the security entitlement, or bulk purchasers of the assets of an entitlement holder. Id. at 717; see infra note 130 (defining “repo” lending). A more in-depth review of the differing applications of these provisions is beyond the scope of this Article. Suffice to say, while these two alternative purchaser protection provisions may apply instead of section 8-502, it stands to reason that the relevant legal analysis would be substantially the same.

83. Hakes, supra note 47, at 686 (noting that the drafters of the 1994 revisions were clear in their intent that the property rights of an entitlement holder were created by Article 8 and not by common law property concepts).

84. Id. at 710–11 (discussing the “three unique rules to protect [subsequent] purchasers” that the drafters implemented in the 1994 revisions).

85. Id. at 713–14.

86. Id. at 674–75.

87. Id. at 676.
common law requires.\textsuperscript{88} “In the extreme, an entitlement holder could acquire a security entitlement with knowledge that the financial asset was subject to numerous significant claims and still be protected from a particular claim, because it did not happen to have notice of that claim.”\textsuperscript{89} On this understanding, Article 8 would seem, at face value, to provide adequate protection to any subsequent purchaser of a security that had been stolen in a cyber attack.

However, notwithstanding the language of Article 8 and the drafters’ clear intent, it is questionable how rigorously courts would protect a subsequent purchaser’s securities entitlements. Consider the following hypothetical scenario.

An investor’s (the “original owner” or entitlement holder) account at Morgan Stanley (the “financial intermediary”) is hacked, and his IBM shares are transferred to Hacker’s account at JP Morgan. Hacker then puts in a sell order. Simultaneously, B Brokerage House (the “transferee intermediary”) buys IBM shares from JP Morgan to satisfy its customers’ buy orders for the day. Hacker’s account at JP Morgan is then credited cash, which is instantaneously transferred to an offshore account, and the IBM shares are transferred to B Brokerage House and to a Buyer’s (the “subsequent purchaser”) account there, which is credited with the stolen IBM securities and debited the cash.

After such a hack and resale, how would courts sort out the ownership rights to the IBM securities between the original entitlement holder and the subsequent purchaser/buyer? The uncertainty is troubling: A failure to maintain the purchaser’s rights, as Article 8 envisions, would lead to the pernicious effects on the markets discussed above—that is, exacerbated investor fear of trading, liquidity, and credit problems. The next Section of this Article explores these possibilities.

\textbf{B. Judicial Interpretations of Article 8’s Purchaser Protections}

As commentators have noted, Article 8 is not a well understood area of law, even among commercial law experts.\textsuperscript{90} It appears that “[t]he operations of the modern book-entry system are not matters within the

\textsuperscript{88} Id. at 714.
\textsuperscript{89} Id. (emphasis added).
\textsuperscript{90} Rogers, supra note 2, at 1432 (“Article 8 is one of the more recondite branches of commercial law. Neither the generalist practicing lawyer nor the commercial law expert is likely to feel comfortable with this subject. Article 8 is not commonly taught in law school commercial law courses and is omitted or given scant coverage in the principal secondary sources on commercial law.”).
daily experience of ordinary lawyers, law professors, legislators, or judges.” Given this lack of familiarity in the bench and bar, it stands to reason that, if faced with investor suits arising from a cyber attack, courts might overlook—or eschew—the purchaser protections embedded in Article 8 and instead rely on more malleable (and familiar) common law principles. Though courts may be inclined toward such an approach, it would give short shrift to the purchaser protections that the drafters intended, undermining their efforts to supersede the common law and prevent market destabilization in times of financial strain.

The following discussion demonstrates how judicial misinterpretations of Article 8 might chip away at the four layers of purchaser protection the drafters intended and considers the resulting consequences.

1. Asserting a Claim: Burden-shifting and Proving an “Adverse Claim”

As noted, Article 8 states as a prerequisite to “any action” that there be an “adverse claim.” The burden is on the claimant (the original owner/entitlement holder) to prove this as part of his prima facie case. However, given the nature of the indirect holding system, this is nearly impossible for any investor to do. In the majority of cases, an investor whose securities had been stolen by a hacker would not have a “claim” against anyone, except his financial intermediary. As discussed, the rights of an entitlement holder against transferees of securities (i.e., subsequent purchasers) are drastically curtailed under Article 8. The principal, if not exclusive, avenue for recourse is against the financial intermediary. As Hakes explains, “section 8-116 makes the securities intermediary, not the entitlement holder, the ‘purchaser for value’ of the financial asset.” Thus, it is the financial intermediary who would have the “adverse claim” and, therefore, would have to be the one to assert those rights against a third-party purchaser.

In the context of a large-scale hack, barring all investors from filing suit in this way might strike many courts as unfair or contrary to public

---

91. *Id.*
92. *Id.* at 1436.
93. U.C.C. § 8-502 (1994); see also Hakes, *supra* note 47, at 675–76 (describing the 1994 revisions to Article 8).
95. *Id.* at 689.
96. However, if the financial intermediary is insolvent and cannot satisfy its customers’ claims, then a claim accrues in favor of the original owner, the investor. Then, he too has a proper “adverse claim” against the transferee-intermediary and/or the subsequent purchaser. Financial intermediaries have a duty under U.C.C. section 8-504 to maintain sufficient interests in the relevant financial asset to satisfy all of its outstanding security entitlements.
policy. It is thus unclear whether courts would actually maintain the legal fictions of the indirect holding system and preclude investors from bringing claims against subsequent purchasers, particularly if there were a large number of victimized investors and the power disparity between investors and financial institutions inspired the courts to exercise their discretion to depart from the letter of section 8-502.

2. Notice: Good Faith and Constructive Notice

Whether a subsequent purchaser of securities qualifies for the protected purchaser status of Article 8 turns on whether the subsequent purchaser had “notice of the adverse claim.” As discussed, another way in which the 1994 revisions attempted to enhance the protections afforded to subsequent purchasers was by making it more difficult to prove that a purchaser had such notice. It did this in two ways. First, the revisions dispensed with the requirement of good faith. Second, they eliminated the concept of constructive notice and affirmatively limited the ways in which a subsequent purchaser could be found to have had notice of an adverse claim to actual notice, willful blindness, or by statutory duty.

Nonetheless, it appears as though some courts remain attached to these common law principles of constructive notice and good faith in forming their judgments about notice under Article 8. As others have noted, it is not uncommon for courts to strain to apply familiar common law principles when faced with unpalatable provisions in the U.C.C., particularly where a

97. U.C.C. § 8-502 (1994). Technically speaking, there is a slight difference in the legal standards to which an intermediary and an individual investor would be held. An intermediary bears the burden of proving it has not acted “in collusion with” the transferor (the hacker). Id. § 8-503(e). In contrast, a subsequent purchaser must prove he purchased the securities “without notice” of the adverse claim. Id. § 8-502. Some commentators have argued that the “collusion” and “notice” standards are, in practical application, indistinguishable. See Rogers, supra note 2, at 1533–37. Others have claimed that the “collusion” standard in section 8-503 is even laxer than the notice standards in sections 8-502 and 8-510. Id. at 1536–37. The latter theory is interesting in light of the fact that the collusion standard applies to secured purchasers and repo lenders, the parties who provide credit to the securities industry. See Hakes, supra note 47, at 721–22. Regardless, for ease of reference, the balance of this Article considers the “collusion” standard the same as “notice.”

98. See Hakes, supra note 47, at 675–78. Strictly speaking, because the 1977 version did not have a section dedicated to the indirect holding system analogous to the current section 5, the concepts of good faith and constructive notice were “eliminated” only from section 8-303—the new section 5 simply never incorporated those principles into its purchaser protection rules in the first place.

99. U.C.C. § 8-105(a) (1994); see Hakes, supra note 47, at 676 (discussing requirement for notice of an adverse claim).
claimant presents a sympathetic case. At least in New York, where a significant proportion of hack-related suits would likely be litigated, there is good reason to think that courts would continue to rely on the more flexible common law principles in the context of investor suits arising from a cyber attack.

For instance, in *MCC Proceeds, Inc. v. Advest, Inc.*, the First Department of the Appellate Division discussed the subjective basis for establishing notice under the New York Commercial Code, which is “knowledge of such facts that ... [the investor’s] action in taking the security amounts to bad faith.” In that discussion, the court noted that such basis for finding notice is “not materially different from” a requirement of good faith. The court in *MCC* went on to suggest that principles of constructive notice might also continue to guide courts’ notice analysis. It stated that, in addition to the subjective component to notice, there is also an objective component, which considers whether “the circumstances known to the purchaser are so obviously suspicious that no honest person (not just a reasonably prudent person) could turn a blind eye thereto.” Such circumstances would require “the purchaser ... [to] investigate.” How far and deeply would courts require a purchaser to “investigate” in the context of a hack?

Other cases have suggested that good faith and constructive notice continue to be relevant to notice, even after the 1994 revisions. For instance, while applying New York state law, the Second Circuit in *SEC v.

---

100. Hakes, *supra* note 47, at 678 (noting that “[t]here is support for the notion that courts deciding cases involving the indirect holding of securities applied whatever principles were necessary to protect innocent investors”); Schroeder, *supra* note 46, at 336 (noting how, under an earlier version of Article 8, courts avoided legal fictions of the U.C.C. and instead applied “more familiar traditional property” rules).

101. See Hakes, *supra* note 47, at 706–07. Hakes explains that “[t]he choice of law rules in Article 8 mandate that the local law of the securities intermediary’s jurisdiction governs adverse claims to security entitlements and the securities intermediary’s duties to adverse claimants.” *Id.* at 706. He further argues that the choice of law should be determined by “the jurisdiction in which the securities intermediary’s chief executive office is located.” *Id.* at 707. Given that the majority of financial institutions are located in New York City, it stands to reason that New York law would govern in a significant number of these cases.


103. 743 N.Y.S.2d 1 (App. Div. 1st Dep’t 2002). Notably, however, the court here applied the U.C.C. in effect in 1991—not the version that New York adopted with the 1997 revisions. *Id.* at 4 (applying the version of U.C.C. section 8-302(1) that was “in effect during the relevant period”).

104. *Id.* at 5 (quoting U.C.C. § 8-304(4) (1991)).

105. *Id.*

106. *Id.*

107. *Id.*
Credit Bancorp, Ltd.\textsuperscript{108} seemed to use those principles to inform its willful blindness analysis.\textsuperscript{109} There, the issue was whether an intermediary (Deutsche Bank) was on notice of adverse claims to securities it held as collateral for one of its customers (CBL) where press releases and various letters had referred to claims to those securities arising from CBL’s perpetration of a Ponzi scheme.\textsuperscript{110} In finding that Deutsche Bank had notice, the court quoted with approval the test proffered by that bank, stating that “the proper test is whether [the bank] ‘deliberately closed [its] eyes to some easily obtained information’ or exhibited ‘subjective bad faith and dishonesty.’ ”\textsuperscript{111}

The authority that exists on Article 8’s notice element, though slim, suggests that courts will rely on principles of good faith and constructive notice (at least in New York), notwithstanding Article 8’s efforts to reject these requirements. Based on this authority, New York courts could very well require an investor to have inquired—with significant diligence—into the provenance of a security that he purchased to determine whether some of those securities had been hacked and stolen at one time or another.\textsuperscript{112}

Courts would no doubt be encouraged to take this approach by the body of familiar case law dealing with another type of stolen property, art. In New York at least, art law resoundingly favors the original owner and is reluctant to find any subsequent purchaser of stolen art to be a bona fide purchaser. The case of Menzel v. List\textsuperscript{113} is a prime example. There, the plaintiff brought a replevin claim to recover a painting by Marc Chagall that the Nazis had stolen from her and her husband’s Brussels apartment in

\textsuperscript{108} 386 F.3d 438 (2d Cir. 2004).
\textsuperscript{109} Id. at 447–48. The court here applied the protected purchaser rule found in section 8-510.
\textsuperscript{110} Id.
\textsuperscript{111} Id. at 452 (quoting SEC v. Lehman Bros., Inc., 157 F.3d 2, 6–7 (1st Cir. 1998)).
\textsuperscript{112} But see Scher Law Firm v. DB Partners I LLC, No. 14515/2006, 2011 WL 322481, at *14–17 (N.Y. Sup. Jan. 28, 2011) (declining to find notice based on a theory of willful blindness). However, the court’s extensive discussion of the facts of the case reveals that the relevant respondent actors did not have notice of the adverse claims against the security interests (collateral) at issue. See id. Importantly, however, the opinion left open the possibility that deliberate avoidance or willful blindness might be found if there were compelling “evidence presented that the [respondent] Bank’s standard diligence procedures were ineffective or that any Bank employee deliberately suppressed, avoided or disregarded information that should have aroused their suspicions.” Id. at *48. Furthermore, U.C.C. section 8-510(a) imposes a duty of due diligence in the presence of suspicious circumstances surrounding a transaction. What constitutes “suspicious circumstances” in the context of a hack could arguably be given broad interpretation by the courts.
\textsuperscript{113} 267 N.Y.S.2d 804 (Sup. Ct. 1966).
After the war, the painting made its way to Paris, and then eventually into the hands of an established New York art dealer. The dealer then sold the piece to a reputable collector, Albert A. List. The court denied List’s motion to dismiss and showed little sympathy for List’s good faith claim, underscoring that “the principle has been basic in the law that a thief conveys no title as against the true owner.” The Menzel rule was reaffirmed in 1991 in Solomon R. Guggenheim Foundation v. Lubell, which confirmed the staunchness with which New York law protects the original owner. It reasoned:

[O]ur decision today is in part influenced by our recognition that New York enjoys a worldwide reputation as a preeminent cultural center. To place the burden . . . on the true owner and to foreclose the rights of that owner to recover its property[,] . . . we believe, [would] encourage illicit trafficking in stolen art. . . . In our opinion, the better rule gives the owner relatively greater protection and places the burden of investigating the provenance of a work of art on the potential purchaser.

Applying such reasoning to the securities context is tempting. As in art, New York also enjoys preeminence in the securities market. Courts might, therefore, be attracted to a rule that places the burden on the subsequent purchaser of stolen securities, on the theory that such a rule would reduce the liquidity of stolen securities and deter hacking.

However, holding investors to requirements of good faith and constructive notice would make it very difficult for a subsequent purchaser of securities to establish that he lacked notice of an adverse claim. As discussed, that outcome would work at cross-purposes to the Article 8 revisers’ intent. After all, any cyber attack would be widely publicized, presumably putting every potential investor on notice that transacting in the compromised security involves an adverse claim from someone.

3. Proving a Specific Adverse Claim

Finally, the literal language of section 8-502 appears to require a claimant to trace his claim to the particular securities stolen and illegally

---

114. Id. at 806.
115. Id. at 806–09.
116. Id. at 807.
117. Id. at 819.
119. Id. at 430.
120. Id. at 431.
transferred. However, because of the indirect holding system, which lumps securities in fungible bulk on the books of intermediaries who net trades each day, “any traditional principles of tracing in the case of investment securities may be theoretically, as well as practically, impossible.”

Given the practical impossibility of tracing individual securities entitlements, the adverse claimant, if held to that requirement, would almost never be successful in stating its claim.

Again, it is quite possible that courts will find the actual operation of these protections—as cutting off the adverse claimant—untenable and unfair, especially in the face of a large-scale cyber theft. As Professor Schroeder has found in similar Article 8 contexts, courts have nearly always rejected the fungible bulk fiction that creates these tracing problems to find that cases “involved identifiable securities that were traceable to specific identifiable purchasers.”

4. The Consequences of Uncertainty: Inefficiency and “Chilling”

While favoring an original (entitlement holder) owner whose securities have been stolen in a hack might have some surface appeal of fairness, doing so would be a shortsighted and market-destabilizing approach.

As a general matter, the disconnect between the literal language of Article 8 and courts’ interpretations thereof would create investor uncertainty, thus increasing inefficiencies in the securities markets. It is a basic economic principle that uncertainty prompts risk-averse actors to “take more than the optimal level of care”—that is, to over comply with the law. As Calfee and Craswell explain, this extra care may be thought of as an externality. Admittedly, overcompliance might not be much of a concern in some settings; for instance, a driver who exercises “too much” care on the road, although perhaps frustrating, does not present a particularly troubling social or economic outcome. By contrast,
overcompliance in the securities context could lead to two undesirable effects: deflated prices and the chilling of securities transactions.

For one, price inefficiencies will likely result from an influx of irrelevant information, worry, and added effort into the process of buying and selling securities that have been compromised by a hack. If investors exert unnecessary time and effort into researching the provenance of a security before purchasing it, that extra effort will adversely impact the price of the security. These price fluctuations are inefficient because they reflect effort and information that are not necessarily relevant to the value of the company; in other words, the stock’s price will incorporate “noise.” Not only might the value of a stock become inappropriately undervalued, but also transaction costs and fees associated with that security could become inappropriately inflated. To return once more to the art analogy, that market has experienced a similar problem. There, “[b]ecause the markets in certain artifacts have become so inundated with forgeries, purchasers are willing to pay an enormous premium for the rare examples with an established provenance”—or, stated differently—pay less for those that do not.\(^\text{127}\) The secondary effects of a deflated share value would include an increase in the cost of capital to the firm, a resulting reduction in hiring and project capacity in the industry, and, more broadly, slower economic growth.

A second byproduct of overcompliance is the chilling of socially desirable behavior.\(^\text{128}\) In this context in particular, economically desirable securities transactions could be chilled as a result of investor overcompliance (that is, risk aversion) vis-a-vis Article 8’s notice requirement. This chilling effect might happen in one of two ways. First, judicial solicitude for original owners’ rights might worsen investor anxiety. In the face of courts’ reluctance to protect their rights, investors are likely to be nervous about their exposure to compromised securities. Naturally, sensing the risks involved, many investors will steer clear of securities that are perceived to be tainted by a hack. Alternatively, if the courts’ behavior encourages original owners to bring suit against subsequent purchasers to recover the value of their securities, these suits could so cloud the title to the securities entitlements that the negotiability of any given stock would be drastically reduced.\(^\text{129}\) As a result, investors


\(^{129}\) See Schroeder, \textit{supra} note 46, at 476.
will be further discouraged from buying securities over which there are (or could be) ownership disputes.

Given the rapidity with which the market operates, once the price of a hacked stock falls, because investor demand has dried up (or “chilled”), the downward spiral of that stock’s value will be hard to curtail. If more than one company’s stock is stolen in a hack or series of hacks, the long-term market effects could be much more serious. If transacting in those securities continues to be chilled, as the securities’ values drop, a fear of lending—not just buying—could set in, reducing the availability of credit and, much as in 2008, another credit crisis could ensue.

C. An Alternative Approach

In light of the foregoing discussion, it is time for additional revisions to Article 8. Just as the 1994 revisions were motivated by developments in the settlement and clearing processes, perhaps another round of revisions is called for in response to the new technological threats those processes and to investor rights in general. After all, the impetus for the last round of revisions was concern for the safety and efficiency of the settlement system, as well as the recognition that outdated commercial law rules can be a destabilizing factor in times of financial stress. Thus, the prospect of

130. This is because many investors have springing sale orders that are automatically triggered by a drop in price below a certain level. See, e.g., Combine Orders, Program Trades and Set Stop Parameters, AMERITRADE, https://www.tdameritrade.com/tradingtools/advanced.html (last visited Mar. 22, 2012) (discussing options for “Trade Triggers” and “Trailing Stops”). In addition, securities are also used as collateral for short-term loans. Known as “repo lending,” this source of short-term liquidity is critical to the operation of modern financial institutions:

A “repo” is the sale of a security accompanied by the seller’s agreement to repurchase the security at a later time for the original purchase price plus a differential that equates to interest between the dates of the sale and repurchase. If the security itself pays interest or dividends between the dates of the sale and repurchase, the purchaser pays them over to the seller.


131. The genesis of the 2008 financial crisis and credit crunch was the collapse of subprime-backed securities, which forced banks to absorb large losses. These losses—and the fear of further loss—prompted those institutions to become highly risk averse, meaning that they became increasingly reluctant to offer other institutions, companies, and households credit. See Ni, supra note 43, at 241–42 (“The heightened risk aversion spread from money markets to almost every corner of the credit markets.”).

132. Rogers, supra note 2, at 1436.
additional revision is not at all far-fetched, particularly once the commercial law community fully considers the risks discussed above.

One option is to revise Article 8 to include an indemnity provision that operates in the context of cyber attack. This new provision could provide subsequent investors (purchasers) with complete indemnification from adverse claims, with no required showing of a lack of notice. Of course, indemnification rights should be refused in instances of actual, obvious knowledge, but, barring that, courts would not be permitted to reach the question of notice at all, avoiding the temptation to consider good faith, constructive notice, or some expanded version of willful blindness. Stated simply, under a clear indemnification rule, a plaintiff would fail to state an adverse claim unless able to show actual notice.

Critics of this bright-line rule will likely argue that it is too dismissive of the original owners’ property rights, who will have lost their securities and will be limited to recourse against their intermediary. However, the beneficial incentive effects of an indemnification rule outweigh that downside.

With an indemnification rule in place, investors would be incentivized to take more care in selecting the financial intermediary with whom they place their securities. Greater investor attention to information and data security will naturally incentivize financial intermediaries to invest more resources in fortifying their systems against hacks and other cybercrimes. This consumer-driven accountability could be significant in avoiding or mitigating the risk of hacks in the first instance. In short, an indemnification rule incorporated into Article 8 would not only stave off market-freezing effects in the event of a hack, but would also engender greater information security accountability in the U.S. financial sector.

As a general matter, others have also recognized the need for greater information security accountability in the finance industry. One scholar has suggested oversight mechanisms such as increased SEC regulation, a

---

133. See Schroeder, supra note 46, at 299 (commenting that many may find aspects of the 1994 revisions, which provide additional protections to subsequent purchasers held through broker-dealers, “repugnant either on the ethical grounds that it rewards thieves . . . or on the political, economic or philosophical grounds that it insufficiently protects property rights, or both”). A related criticism is that setting a lower bar for bona fide purchaser (or protected purchaser) status raises ethical concerns, as it may incentivize “disreputable” behavior on the part of transferees and undermine confidence in the integrity of the market. Id. at 490–91.

134. Article 8 provides recourse against the intermediary that fails to fulfill its statutory obligations, which might be interpreted to include the duty to provide reasonably sufficient protection against security breaches. See Hakes, supra note 47, at 696 (describing the intermediary’s obligations to the entitlement holder to exercise due care under U.C.C. sections 8-504(c)(1)–(2), 8-505(a)(1)–(2), 8-506(1)–(2), 8-507(a)(1)–(2), 8-508(1)–(2), and 8-509).
requirement for chief information officers in all public companies and financial services providers, and materiality standards for disclosing data breaches. As that scholar argues, “[t]he SEC must take a more aggressive lead in creating a culture of information accountability in our markets.” Indeed, federal regulation in other online data privacy contexts is already well established. For example, the Gramm-Leach Bliley Act (“GLBA”) imposes “an affirmative and continuing obligation” on financial institutions to, inter alia, “protect the security and confidentiality of those customers’ nonpublic personal information.” Also, the Federal Deposit Insurance Corporation (“FDIC”) requires financial institutions to develop plans to safeguard customer information, particularly with regard to the use of electronic banking systems. Similar oversight and regulation mechanisms tailored to the context of investment securities transactions would be the ideal complement to an Article 8 revision.

CONCLUSION

This Article has demonstrated the likelihood of a cyber attack in the U.S. securities markets and explored the market-wide consequences that would follow such an attack. The current law, as applied, creates a worrisome picture for any investor considering purchasing securities after a hack attack. That fear and anxiety would have serious, detrimental effects on our capital markets and economy. However, an indemnification rule incorporated into Article 8 could go far in not only mitigating market destabilization but also avoiding a hack in the first place.

135. Matwyshyn, supra note 1, at 586, 592–93.
136. Id. at 594.