



TOURO UNIVERSITY
JACOB D. FUCHSBERG LAW CENTER
Where Knowledge and Values Meet

Touro Law Review

Volume 33 | Number 2

Article 11

2017

Computer Systems Fraud - Computer Systems Fraud in the Era of Big Data and EHRs

John Sepulveda

Follow this and additional works at: <https://digitalcommons.tourolaw.edu/lawreview>



Part of the [Contracts Commons](#), and the [Insurance Law Commons](#)

Recommended Citation

Sepulveda, John (2017) "Computer Systems Fraud - Computer Systems Fraud in the Era of Big Data and EHRs," *Touro Law Review*. Vol. 33: No. 2, Article 11.

Available at: <https://digitalcommons.tourolaw.edu/lawreview/vol33/iss2/11>

This Article is brought to you for free and open access by Digital Commons @ Touro Law Center. It has been accepted for inclusion in Touro Law Review by an authorized editor of Digital Commons @ Touro Law Center. For more information, please contact lross@tourolaw.edu.

**COMPUTER SYSTEMS FRAUD - COMPUTER SYSTEMS
FRAUD IN THE ERA OF BIG DATA AND EHRs**

*John Sepulveda**

**COURT OF APPEALS OF NEW YORK
UNIVERSAL AMERICAN CORP. v. NATIONAL UNION FIRE
INS. CO. OF PITTSBURGH, P.A.¹**

I. INTRODUCTION

In *Universal American Corp. v. National Union Fire Ins. Co.*,² the New York Court of Appeals found that a rider for indemnification for losses due to computer systems fraud covers only the unauthorized use of the computer system and not fraudulent use by an authorized user.³ Universal American Corporation, a health insurance company, sought to indemnify itself from losses due to computer systems fraud by purchasing an insurance agreement from National Union Fire Insurance Company.⁴ The contract provided for coverage against losses incurred by an unauthorized user of the insured's computer system who commits fraudulent acts.⁵ Within only a few months after purchasing this insurance agreement, Universal suffered losses from authorized users inputting fraudulent

*J.D. Candidate 2017, Touro College Jacob D. Fuchsberg Law Center; M.B.A., Dowling College, 2002; B.S. in Electrical Engineering Technology, SUNY Farmingdale, 1997. I would like to thank my devoted wife Ania and beloved daughter Alexandra, for all their support and love, without you this would not be possible. Special thanks to my parents John and Mildred for their support and guidance. Thanks to Julie Ansanelli and Jessica Vogeles for helping me find my voice. Finally, Dean Rodger Citron, who has provided me guidance and encouragement throughout.

¹ 37 N.E.3d 78 (N.Y. 2015).

² *Id.*

³ *Id.* at 79.

⁴ *Id.*

⁵ *Id.*

data into Universal's computer system.⁶ The Court of Appeals considered whether the insurance agreement for computer systems fraud applied to "a fraudulent entry . . . of Electronic Data or Computer Program" caused by an authorized user's fraudulent acts.⁷ It found that the contract precluded coverage for such losses, as the contract covered only the unauthorized use of the computer system.⁸ The Court of Appeals' holding in *Universal* alerts health insurance companies seeking to indemnify themselves against these kinds of losses that they should seek additional advice as to whether their current computer systems fraud rider offers the coverage they seek. The court's holding in *Universal* also signals that health insurers should also explore obtaining other insurance policies and additional coverage.

This case note will primarily discuss the decision in *Universal*, in which the Court of Appeals interpreted a rider for indemnification losses due to computer systems fraud to cover only unauthorized use of the system. Ultimately, this case note will suggest that health insurance providers should purchase riders on their insurance policies that cover these losses. This case note is divided into five parts. Part II will outline the relevant facts, procedural history, and the Court of Appeals' holding in *Universal*. Part III will analyze the various standards for fraudulent use and unauthorized users when dealing with computer fraud. Part IV will discuss Universal's possible remedies, which include various criminal and civil penalties against the providers that committed the fraud. Part V will make recommendations regarding insurance contract provisions for the health care insurance industry to help mitigate the losses associated with computer-based insurance fraud.

II. UNIVERSAL AMERICAN CORP. V. NATIONAL UNION FIRE INSURANCE CO. OF PITTSBURGH, PENNSYLVANIA

The Court of Appeals in *Universal* found that a rider indemnifying the insured for losses from computer systems fraud covered only unauthorized use of the computer system and precluded coverage for losses incurred by an authorized user.⁹ The following

⁶ *Universal*, 37 N.E.3d at 79.

⁷ *Id.*

⁸ *Id.*

⁹ *Id.*

section will discuss the factual background, the procedural history, and the Court of Appeals' discussion in *Universal*.

A. Factual Background

Universal American Corp. ("Universal") is a health insurance company that provides "Private Fee-For-Service" plans under Medicare Advantage or "Medicare Part C."¹⁰ Medicare Advantage plans, in general, are government-regulated programs of managed health care that allow patients who are eligible for Medicare to purchase health insurance from private companies like Universal.¹¹ The most common types of Medicare Advantage Plans are HMOs (Health Maintenance Organizations), PPOs (Preferred Provider Organizations) and PFFS (Private-Fee-for-Service) plans.¹² Patients with an HMO Plan are required to use health care providers in their network in order to have their care covered by the plan.¹³ On the other hand, patients covered under a PPO Plan may use health care providers outside of the network but may be required to pay more to do so.¹⁴ Finally, patients covered under a "Private Fee-For-Service" plan, like the one provided by Universal, can use their own health care provider, who then submits claims to the insurance company for

¹⁰ *Id.*

¹¹ Informational Brochure, U.S. Dep't of Health and Human Services, *How Medicare Advantage Plans Work*, <https://www.medicare.gov/sign-up-change-plans/medicare-health-plans/medicare-advantage-plans/how-medicare-advantage-plans-work.html> (last visited Feb. 10, 2017).

¹² Informational Brochure, U.S. Dep't of Health and Human Services, *Different types of Medicare Advantage Plans*, <https://www.medicare.gov/sign-up-change-plans/medicare-health-plans/medicare-advantage-plans/types-of-medicare-advantage-plans.html> (last visited Feb. 10, 2017).

¹³ Informational Brochure, U.S. Dep't of Health and Human Services, *Health Maintenance Organization (HMO) Plan*, <https://www.medicare.gov/sign-up-change-plans/medicare-health-plans/medicare-advantage-plans/hmo-plans.html> (last visited Feb. 10, 2017).

¹⁴ Informational Brochure, U.S. Dep't of Health and Human Services, *Preferred Provider Organization (PPO) Plans*, <https://www.medicare.gov/sign-up-change-plans/medicare-health-plans/medicare-advantage-plans/preferred-provider-organization-plans.html> (last visited Feb. 10, 2017).

the health care services rendered.¹⁵ The Department of Health and Human Services reimburses the insurer for those services.¹⁶

Universal utilizes a “computerized billing system that allows health care providers to submit claims directly to the system.”¹⁷ Universal’s computer system automatically processes, approves, and pays the claims without first checking the authenticity of these claims.¹⁸ Universal purchased insurance coverage for a variety of losses from National Union Fire Insurance Co. of Pittsburgh, Pennsylvania (“National Union”), which is a provider of commercial and personal insurance coverage.¹⁹ Within only a few short months of obtaining coverage, Universal suffered more than \$18 million in losses for fraudulent claims for health care services entered into Universal’s computer system that were never actually performed.²⁰ These fraudulent claims proliferated due to Universal’s automated computer system, which allowed health care providers to automatically receive their fee after entering their claims without any check to determine whether their services were actually performed.²¹ Universal sought payment from National Union for these losses.²² National Union denied coverage to Universal and claimed that the contract rider did not cover these losses.²³ Specifically, National Union argued that these losses were standard insurance fraud and not the kind of “computer fraud” covered by the contract rider, which only covered losses resulting directly from “fraudulent . . . entry of Electronic Data” by unauthorized users.²⁴ The contract rider reads as follows:

Computer Systems Fraud

Loss resulting directly from a fraudulent

¹⁵ Informational Brochure, U.S. Dep’t of Health and Human Services, *Private Fee-for-Service (PFFS) Plans*, <https://www.medicare.gov/sign-up-change-plans/medicare-health-plans/medicare-advantage-plans/private-fee-for-service-plans.html> (last visited Feb. 10, 2017).

¹⁶ *Universal*, 37 N.E.3d at 79.

¹⁷ *Id.*

¹⁸ *Id.*

¹⁹ *Id.*

²⁰ *Id.* at 80.

²¹ *Universal*, 37 N.E.3d at 79.

²² *Id.* at 80.

²³ *Id.*

²⁴ *Id.* at 79-80.

(1) entry of Electronic Data or Computer Program into, or
 (2) change of Electronic Data or Computer Program within
 the Insured's proprietary Computer System or a
 Computer System listed in the Schedule below; . . .

provided that the entry or change causes
 (a) Property to be transferred, paid or delivered,
 (b) An account of the Insured, or of its customer, to be
 added deleted, debited or credited or
 (c) An unauthorized account or a fictitious account to
 be debited or credited.²⁵

The Computer Systems Fraud Rider contained several exclusions:

(B) loss resulting directly or indirectly from
 negotiable instruments, securities, documents or other
 written instruments which bear a forged signature, or
 are counterfeit, altered or otherwise fraudulent and
 which are used as source documentation in the
 preparation of Electronic Data or manually keyed into
 a data terminal.²⁶

(D) loss resulting directly or indirectly from the input
 of Electronic Data into a Computer System terminal
 device either on the premises of a customer of the
 Insured or under the control of such a customer by a
 person who had authorized access to the customer's
 authentication mechanism.²⁷

(E) loss resulting directly or indirectly from the theft
 of confidential information.²⁸

In other words, the subtitle, "Computer Systems," covers the insured
 for losses resulting directly from entry of electronic data into
 Universal's computer system, provided that the entry or changed data

²⁵ *Id.* at 79.

²⁶ Brief for Defendant-Respondent at 46-47, *Universal American Corp. v. National Union Fire Insurance Company of Pittsburgh, P.A.*, 2014 WL 10049066 (2014) (No. 2014-00133).

²⁷ *Id.* at *17-18.

²⁸ *Id.* at *51.

causes Universal to pay for a service.²⁹ Next, under “Exclusions,” the rider expressly does not cover losses resulting directly or indirectly from fraudulent negotiable instruments bearing a false signature used as source documentation or from the input of electronic data on the premises of a customer of the insured by an authorized person or “from the theft of confidential information.”³⁰ Universal sued National Union for damages and declaratory relief because National Union refused to cover Universal’s losses.³¹

B. Procedural History

Universal brought an action against National Union for breach of the contractual provision insuring against losses caused by computer systems fraud.³² Universal moved for summary judgment, arguing that the policy covered losses caused by fraudulent entry of claims which were never provided.³³ National Union then cross-moved for summary judgment³⁴ on the grounds that the insurance policy was intended to insure only against losses due to computer hackers or unauthorized users.³⁵

The Supreme Court of New York County held that the language of the rider did not support Universal’s interpretation of the contract, denying Universal’s motion and granting National Union’s cross-motion.³⁶ Universal appealed the trial court’s dismissal.³⁷ The First Department affirmed as modified, and Universal appealed further to the New York Court of Appeals.³⁸

The New York Court of Appeals affirmed as well because it rejected Universal’s argument that an insurance agreement for computer systems fraud that applied to “a fraudulent entry of Electronic Data or Computer Program” encompasses the losses caused by an authorized user’s submission of fraudulent data into

²⁹ *Id.* at *6-7.

³⁰ *Id.* at *5.

³¹ *Universal*, 37 N.E.3d at 80.

³² *Universal American Corp. v. National Union Fire Insurance Company of Pittsburgh, P.A.*, 38 Misc. 3d 859, 860 (Sup. Ct. N.Y. Cnty. 2013).

³³ *Universal*, 37 N.E.3d at 80.

³⁴ *Id.*

³⁵ *Universal*, 38 Misc. 3d at 862.

³⁶ *Universal*, 37 N.E.3d at 80.

³⁷ *Id.* at 79.

³⁸ *Id.* at 80.

Universal's system.³⁹ The court held that the agreement was "unambiguous and 'fraudulent entry' refers to unauthorized access into [Universal's] computer system and not to content submitted by authorized users."⁴⁰

C. The Court of Appeals' Reasoning

In *Universal*, the New York Court of Appeals noted that "an insurance agreement is subject to principles of contract interpretation"⁴¹ as a matter of law.⁴² The court also acknowledged that the various provisions in "an insurance contract must be given their plain and ordinary meaning . . ."⁴³ Relying on its previous decision in *Mostow v. State Farm Insurance Cos.*,⁴⁴ the court held that the test for insurance contract ambiguity is "the reasonable expectations of the average insured . . . employing common speech."⁴⁵ In other words, a contract is ambiguous if the ordinary policyholder's reasonable expectations could come to a different understanding of the terms than the insurance company.⁴⁶ The court in *Universal* concluded that the rider's language "unambiguously" applied to losses caused by unauthorized users of Universal's computer system and not to losses resulting from fraudulent entry by an authorized user.⁴⁷

The court examined two features of the rider's language in *Universal*. First, the court found that the subtitle, "Computer Systems," demonstrated that the focus of the rider was on the computer system as opposed to fraudulent content.⁴⁸ Second, under "Exclusions," the rider expressly did not cover losses resulting from fraudulent instruments "which are used as source documentation in the preparation of Electronic Data or manually keyed into a data

³⁹ *Id.* at 79-80.

⁴⁰ *Id.* at 79.

⁴¹ *Universal*, 37 N.E.3d at 80.

⁴² *Id.*

⁴³ *Id.* (citing *Vigilant Ins. Co. v. Bear Stearns*, 10 N.Y.3d 170, 177 (2008), quoting *Vigilant Ins. Co. v. Bear Stearns Cos., Inc.*, 9 N.Y.3d 264, 267 (2007)).

⁴⁴ *Mostow v. State Farm Ins. Companies*, 88 N.Y.2d 321 (1996).

⁴⁵ *Universal*, 37 N.E.3d 81 (citing *Mostow*, 88 N.Y.2d at 327).

⁴⁶ *Mostow*, 88 N.Y.2d at 326-27.

⁴⁷ *Universal*, 37 N.E.3d at 81.

⁴⁸ *Id.*

terminal.”⁴⁹ The court held that losses described under the “Exclusions” subtitle were considered billing fraud, as opposed to the computer fraud, which was covered by the contract rider.⁵⁰ Judge Rivera, writing for the majority, emphasized that if Universal and National Union intended to cover billing fraud, there would have been no reason to exclude content from fraudulent instruments.⁵¹

To assist in determining the intent of the coverage of the contract rider, the Court of Appeals in *Universal* also examined the ordinary definitions of “fraudulent,” “entry,” and “change,”⁵² which the contract rider did not define.⁵³ The court looked to Merriam-Webster, which defines (1) “fraudulent” as “deceit,”⁵⁴ (2) “entry” as “the act of entering” or “the right or privilege of entering,”⁵⁵ and (3) “change” as “to make different” or “alter.”⁵⁶ Based on these definitions, the court concluded that “fraudulent” “qualifies the act of entering or changing data or a computer program.”⁵⁷ The court determined that in order to rise to the level of fraudulence, the actor must have actively changed data or computer code, as opposed to merely using a computer to fraudulently submit claims for services never rendered.

The New York Court of Appeals next examined Universal’s two principal arguments. First, Universal argued that, for the purposes of the rider, “fraudulent entry” and “fraudulent input” had the same meaning, in contrast with National Union’s argument that the two terms did not have the same meaning.⁵⁸ Specifically, since the health care providers that submitted fraudulent claims had inputted fraudulent data, Universal argued that fraudulent entry could only result from the inputting of fraudulent data.⁵⁹ The court disagreed with Universal and held that these terms did not have the same meaning due to the rider’s language, which stated that coverage was limited to “[l]oss resulting directly from a fraudulent (1) entry of

⁴⁹ *Id.*

⁵⁰ *Id.*

⁵¹ *Id.*

⁵² *Universal*, 37 N.E.3d at 81.

⁵³ *Id.*

⁵⁴ *Id.*

⁵⁵ *Id.*

⁵⁶ *Id.*

⁵⁷ *Universal*, 37 N.E.3d at 81.

⁵⁸ *Id.*

⁵⁹ *Id.*

Electronic Data or Computer Program”⁶⁰ As such, treating the terms “fraudulent entry” and “fraudulent input” as synonyms would ignore the application of the remaining language contained in the rider to “Computer Systems Fraud.”⁶¹ This intentional placement of the word “fraudulent” before the word “entry” demonstrated the parties’ intent to have the rider cover use of the computer system through “deceitful and dishonest access.”⁶²

Second, Universal argued that the court should base its decision on the Superior Court of Connecticut’s decision in *Owens, Schine & Nicola, P.C. v. Travelers Casualty and Surety of America*.⁶³ In *Owens*, the court held that the term “computer systems fraud” in a contract “can reasonably be interpreted to encompass fraud committed through a computer.”⁶⁴ There, the plaintiff, Owens, Schine & Nicola, P.C. (“Owens”), purchased an insurance contract from Travelers Casualty and Surety Company (“Travelers”).⁶⁵ The insurance contract in this case included a “Computer Fraud” provision⁶⁶ and also defined computer fraud in its rider as “[t]he use of any computer to fraudulently cause a transfer of Money, Securities or Other Property from inside the Premises or Banking Premises”⁶⁷ In *Owens*, the computer did not cause the actual transfer of funds but instead the fraudster used the computer to send several e-mails, which then tricked Owens into transferring the funds.⁶⁸ Specifically, after the parties exchanged a series of e-mails, the fraudster executed a retainer agreement with Owens.⁶⁹ Owens was then sent a check for \$198,610.00 and was directed by e-mail to deposit the check and wire \$197,110.00 to the fraudster’s South Korean account.⁷⁰ The check was later determined to be fraudulent by Wachovia Bank and was not honored.⁷¹ Owens’ IOLTA account

⁶⁰ *Id.* at 79-81.

⁶¹ *Id.* at 81 (stating “Universal’s proposed interpretation is easily achieved by providing coverage for a ‘loss resulting directly from fraudulent data’”).

⁶² *Universal*, 37 N.E.3d at 81.

⁶³ *Owens, Schine & Nicola, P.C. v. Travelers Cas. and Sur. Co. of Am.*, 2010 WL 4226958 (Conn. Super. Ct. 2010).

⁶⁴ *Universal*, 37 N.E.3d at 81-82 (discussing *Owens*, 2010 WL 4226958 at *1).

⁶⁵ *Owens*, 2010 WL 4226958 at *1.

⁶⁶ *Universal*, 37 N.E.3d at 82.

⁶⁷ *Id.*

⁶⁸ *Owens*, 2010 WL 4226958 at *1-2.

⁶⁹ *Id.*

⁷⁰ *Id.* at *1.

⁷¹ *Id.* at *2.

was debited the \$197,110.00, at which point Owens submitted a claim to Travelers under the Computer Fraud provisions of their insurance policy.⁷² The question became whether, in light of the parties' reasonable interpretation of the terms, the computer, which was not used to input fraudulent data but to send emails that would later induce fraud, was one of the primary factors in causing this computer fraud.⁷³ The court in *Universal* was unpersuaded by Universal's reliance on *Owens*, as *Owens* focused more on whether a computer had been used in such a way to constitute computer fraud.⁷⁴ In *Universal*, the computer was clearly used in a manner that resulted in payment for claims for services that were never provided because all of the fraudulent entries were directly entered by computer into Universal's Computer System.⁷⁵

The Supreme Court of New York County in *Universal* relied primarily on *Morgan Stanley Dean Witter & Co. v. Chubb Group of Insurance Cos.*,⁷⁶ a New Jersey state appellate case regarding the interpretation of a "Computer Systems" insuring agreement.⁷⁷ In *Morgan Stanley*, the insurance company denied coverage, stating that there was no "fraudulent input" because the customer who entered the fraudulent instructions was an authorized user of Morgan Stanley's computer system.⁷⁸ The contract contained a provision that indemnified the insured for losses arising out of the fraudulent input of electronic data.⁷⁹ This provision was subject to an exclusion that explicitly barred loss from an authorized user.⁸⁰ The court held that,

⁷² *Id.*

⁷³ *Universal*, 37 N.E.3d at 82.

⁷⁴ *Id.*

⁷⁵ *Id.* at 79. "The matter before us involves Universal's demand for indemnification to cover losses resulting from health care claims for unprovided services, paid through Universal's computer system." *Id.*

⁷⁶ *Morgan Stanley Dean Witter & Co. v. Chubb Group of Ins. Companies*, 2004 WL 5352285 (N.J. Super. L. 2004).

⁷⁷ *Id.* at *5-6.

⁷⁸ *Id.*

⁷⁹ *Id.* at *2.

⁸⁰ *Morgan Stanley Dean Witter & Co. v. Chubb Group of Ins. Companies*, 2005 WL 3242234, at *3 (N.J. Super. Ct. App. Div. Dec. 2, 2005):

The computer systems insuring agreement was subject to Exclusion (q), which provides that the agreement does not cover 'loss by reason of the input of Electronic Data at an authorized electronic terminal . . . or a Customer Communication System by a customer or other person who had authorized access' Thus, the exclusion, which seems clear and

pursuant to this exclusion, there was no fraudulent input because the customer was an authorized user at an authorized terminal.⁸¹ The court in *Universal* found *Morgan Stanley* instructive because, as in *Universal*, the contract specified that it did not provide coverage for authorized users who entered fraudulent data.⁸²

Ultimately, in *Universal*, the New York Court of Appeals concluded that the contract rider that insured against “Computer Fraud” did not apply to losses from the data submitted by authorized users, even though computers were used to commit fraud; instead, the contract rider only applies to “hacking.”⁸³

III. FRAUDULENT ACTS VERSUS UNAUTHORIZED USERS

An issue that arises from the inclusion of computer systems fraud riders in insurance contracts is whether the party that committed fraud was an otherwise authorized user of the covered computer system at the time he committed the fraudulent act. The New York Court of Appeals in *Universal* might have reached a different conclusion had it considered the following facts with respect to whether the contract rider covered fraud committed by authorized users: (1) the insurance industry defines computer fraud in a manner contrary to the hacker-centric definition provided by the court in *Universal*, (2) authorized users can commit fraudulent acts, (3) the terms “fraudulent” and “unauthorized” are not synonymous, and (4) computer fraud does not require high tech “hacking.”

The hacker-centric definition provided by the court in *Universal* is contrary to the definition used in the insurance industry for computer fraud. The International Risk Management Institute, a major insurance educational organization, defines “Computer Systems Fraud” insurance as covering “loss resulting from fraudulent input or alteration of electronic data or computer programs within the insured’s computer system by a nonemployee.”⁸⁴ This definition is in

unambiguous, excludes coverage for fraud committed by customers or other authorized persons.

Id.

⁸¹ *Id.* at *5.

⁸² *Universal*, 38 Misc. 3d at 863-64.

⁸³ *Universal*, 37 N.E.3d at 81.

⁸⁴ Brief for United Policyholders as Amicus Curiae Supporting Plaintiff-Appellant at 8-9, *Universal Am. Corp. v. Natl. Union Fire Ins. Co. of Pittsburgh, PA.*, 37 N.E.3d 73 (2015) (No. 2014-00133).

line with the definition proposed by Universal, yet is contrary to the Court of Appeals' interpretation.⁸⁵ The Court of Appeals defines computer fraud as "wrongful acts in manipulation of the computer system, i.e. by hackers."⁸⁶ There were no hackers in *Universal*.⁸⁷ The facts instead comport with the International Risk Management Institute's definition because Universal suffered losses resulting from fraudulent input within Universal's computer system by health care providers who were non-employees.⁸⁸ In other words, if the court in *Universal* had used the industry definition, the court would have held that there was computer systems fraud due to the input of fraudulent data by service providers or vendors who were not employees of the insured.⁸⁹

An additional point that the court in *Universal* failed to consider is that an authorized user can commit fraudulent acts. In *Universal*, the Court of Appeals insisted that the two terms were mutually exclusive, which resulted in its characterization of the health care providers as authorized users.⁹⁰ In contrast, the United States District Court, Eastern District Michigan, Southern Division in *United States v. Khan*,⁹¹ held that a user may be authorized and still commit fraudulent acts.⁹² In *Khan*, the health care provider, Amjad Khan, and his associates submitted false claims for health care benefits and services.⁹³ The health care provider in *Khan* was an authorized user but the court nonetheless held that these false claims rose to the level of fraud because Khan, as a health care provider, was authorized to seek reimbursement from Medicare but fraudulently sought this reimbursement by presenting false statements.⁹⁴ Specifically, the health care provider's fraudulent acts included submitting "[f]raudulent entries in cost reports and supporting documentation submitted to Medicare by AHHC."⁹⁵ In *Universal*, the health care insurer similarly received false claims by authorized

⁸⁵ *Universal*, 37 N.E.3d at 81.

⁸⁶ *Id.* at 80.

⁸⁷ *Universal*, 38 Misc. 3d at 861.

⁸⁸ *Id.*

⁸⁹ *Universal*, 37 N.E.3d at 79.

⁹⁰ *Id.*

⁹¹ *United States v. Khan*, 2008 WL 2782669 (E.D. Mich. 2008).

⁹² *Id.* at *1.

⁹³ *Id.*

⁹⁴ *Id.*

⁹⁵ *Id.* at *2.

users for services not provided.⁹⁶ The court should have compared the facts in *Universal* to the facts in *Khan* and then based its decision, at least in part, on the reasoning of *Khan*. Similarly, in *People v. Severino*,⁹⁷ the defendant, a nursing home business manager, made fraudulent entries in applying for Medicaid reimbursement.⁹⁸ There, the defendant fraudulently listed over \$63,000.00 in expenditures as incurred during patient care.⁹⁹ The defendant's wife and son owned the nursing home and employed the defendant there.¹⁰⁰ The New York Appellate Division, Second Department, affirmed the trial court's judgment convicting the defendant of offering a false instrument and grand larceny.¹⁰¹ As in *Universal*, the fraudsters in *Severino* were authorized users of the system.¹⁰² The court in *Universal* should have ruled in *Universal*'s favor because the authorized users in *Universal*, like the authorized users in *Severino* and *Khan*, used the computer system in a fraudulent manner by submitting false claims.

The outcome in *Universal* would have been different had the court not interpreted the words "fraudulent" and "unauthorized" as synonymous. The First Department in *Waters v. Horace Waters & Co.*¹⁰³ held that the terms "fraudulent" and "unauthorized" are not synonymous because an individual can be authorized to do a fraudulent action.¹⁰⁴ In *Waters*, a stockholder brought an action to cancel some shares of treasury stock.¹⁰⁵ The corporation issued the stocks at par value to an older employee and officer of the corporation to ensure his retention.¹⁰⁶ Although stocks were given to the employee-stockholder, she was not offered the opportunity to subscribe to a proportionate part of the three shares.¹⁰⁷ The court

⁹⁶ *Universal*, 37 N.E.3d at 79.

⁹⁷ *People v. Severino*, 63 A.D.2d 1010 (App. Div. 2d Dep't 1978).

⁹⁸ *Id.* at 1010.

⁹⁹ *Id.*

¹⁰⁰ *Id.*

¹⁰¹ *Id.*

¹⁰² *Severino*, 63 A.D.2d at 1010.

¹⁰³ *Waters v. Horace Waters & Co.*, 130 A.D. 678 (App. Div. 1st Dep't 1909) *aff'd*, 201 N.Y. 184 (1911).

¹⁰⁴ *Id.* at 685 (stating "[u]nauthorized acts are not necessarily fraudulent").

¹⁰⁵ *Id.* at 683.

¹⁰⁶ *Id.* at 684.

¹⁰⁷ *Id.* at 684-85.

held that the issuance of the three shares constituted fraud,¹⁰⁸ even though the corporation was authorized to issue them.¹⁰⁹ On the other hand, the court in *Universal* held that the coverage extended only to “wrongful acts in manipulation of the computer system, i.e. by hackers,” not by authorized users.¹¹⁰ Though the health care providers were authorized users of the system, it is arguable that they committed fraudulent acts by making claims for services never rendered. If the court had not interpreted the terms “fraudulent” and “unauthorized” as synonyms, the court may have held similarly to *Waters* on the issue of computer fraud. Such an interpretation is consistent with the plain text of the rider, which covered “[l]oss resulting directly from a fraudulent (1) entry of Electronic Data or Computer Program,” as opposed to the current interpretation as unauthorized entry.¹¹¹

Had the Court of Appeals interpreted the contract provisions not to require a “computer hacking incident” for indemnification against losses, the policy would have covered *Universal* for losses incurred due to fraudulent claim submissions in its computer system. In *Owens*, the court held “that a computer hacking incident” was not a requirement for coverage in a policy indemnifying losses caused by computer fraud.¹¹² No “computer hacking incident” had taken place; instead, the fraudulent act was the direct result of the third party who had communicated with *Owens* electronically.¹¹³ The insured sought coverage under a provision that allowed indemnification for losses due to computer fraud and that required only “the use of any computer” in committing such fraud.¹¹⁴ Similar to the policy in *Universal*, the contract in *Owens* did not use the words “hacking” or “unauthorized user.”¹¹⁵ In *Universal*, the traditional computer hacker did not commit the hacking, and the contract did not use the term hacking; instead, an authorized user caused the fraud by submitting

¹⁰⁸ *Waters*, 103 A.D. at 686. “[T]he issue of the three shares was fraudulent. It was a fraud on the corporation.” *Id.*

¹⁰⁹ *Id.* “The corporation has the right to bring an action to cancel said shares as fraudulently issued . . . [and] is in the control of the trustees who issued the shares.” *Id.*

¹¹⁰ *Universal*, 37 N.E.3d at 80.

¹¹¹ *Id.* at 79.

¹¹² *Owens*, 2010 WL 4226958 at *7.

¹¹³ *Id.* at *8.

¹¹⁴ *Id.* at *7-8.

¹¹⁵ *Id.* at *8.

fraudulent claims within the computer system.¹¹⁶ If the court in *Universal* had interpreted the contract using the same criteria as the court in *Owens*, the contract would have covered Universal for the fraudulent acts, which were the result of providers committing fraud using Universal's computer system.

Ultimately, in light of these cases, the court in *Universal* might have come to a different conclusion had it taken into account that: (1) fraudulent acts can be committed by authorized users; (2) the terms "fraudulent" and "unauthorized" are not synonymous; and (3) computer fraud does not necessarily require hacking—the mere use of a computer in an authorized manner to assist in committing fraud is sufficient. First, the insurance industry defines "Computer Systems Fraud" as covering losses "resulting from fraudulent input . . . within the insured's computer system by a nonemployee."¹¹⁷ In *Universal*, the perpetrators of the fraud were neither employees nor customers; they were service providers or vendors that contracted with Universal.¹¹⁸ Second, authorized users, such as doctors and other health care providers like the ones in *Universal*, can commit fraudulent acts in an insured's system by submitting fraudulent expenditures. An act can be fraudulent and authorized at the same time—merely because users are authorized to use a system does not mean that they are authorized to utilize the system to commit fraud. Although Universal authorized its health care providers to enter claims into its system, Universal did not authorize the submission of fraudulent data in its system.¹¹⁹ Third, the commission of computer fraud does not require traditional hacking of a computer system to commit fraud. In *Universal*, fraudulent acts were the result of providers committing fraud using Universal's computer system.¹²⁰ The fraudulent acts were not the result of traditional "hacking," but by the service providers simply entering fraudulent claims for services that they never provided.¹²¹

¹¹⁶ *Universal*, 37 N.E.3d at 78-80.

¹¹⁷ Brief for United Policyholders as Amicus Curiae Supporting Plaintiff-Appellant at 8-9, *Universal Am. Corp. v. Natl. Union Fire Ins. Co. of Pittsburgh, PA.*, 37 N.E.3d 73 (2015) (No. 2014-00133).

¹¹⁸ *Universal*, 37, N.E.3d at 78-79.

¹¹⁹ *Id.*

¹²⁰ *Id.* at 78.

¹²¹ *Id.* at 80.

IV. HEALTH CARE FRAUD PENALTIES

The Court of Appeals' decision in *Universal*, which confirms that insurance will not cover Universal's losses, leaves Universal with few remaining remedies, all of which require pursuit of the various health care providers that committed the fraud. In *Universal*, the health care providers were authorized users of the insured's system for submitting claims.¹²² Health care insurers such as Universal have the following remedies available against those committing health care fraud: 1) criminal penalties for fraud under Title 18 of the United States Code section 1347;¹²³ 2) both civil and criminal penalties under the Federal False Claims Act, 31 United States Code section 3729, for defrauding the government;¹²⁴ 3) civil and criminal penalties under the New York False Claims Act,¹²⁵ for filing fraudulent claims; 4) civil and criminal penalties under New York Consolidated Laws Social Services Law section 145,¹²⁶ for filing fraudulent claims; and finally 5) a lawsuit in state court alleging fraud.¹²⁷ However, due to the relatively small damages caused by each individual perpetrating fraud, and the high cost of prosecuting those committing the fraud, Universal will have difficulty persuading the government to prosecute these individuals.¹²⁸

A. Criminal Penalties

The criminal penalties against health care providers committing health care fraud allow for prison, fines, and restitution.¹²⁹ Criminal penalties as a remedy are difficult for victims of health care fraud to obtain because criminal prosecution is at the

¹²² *Id.* at 78.

¹²³ See 18 U.S.C. § 1347 (2010).

¹²⁴ 31 U.S.C. § 3729 (2011).

¹²⁵ N.Y. STATE FIN. LAW §§ 187-194 (McKinney 2013).

¹²⁶ N.Y. SOC. SERV. LAW § 145(b) (McKinney 2007).

¹²⁷ See 18 U.S.C. § 1347 (2010); see also 31 U.S.C. § 3729 (2011); N.Y. SOC. SERV. LAW § 145-b (McKinney 2007); N.Y. STATE FIN. LAW §§ 187-194 (McKinney 2013).

¹²⁸ See *Universal*, 37 N.E.3d at 78.

¹²⁹ See 18 U.S.C. § 1347(a)(1) (2010); N.Y. SOC. SERV. LAW § 145-b (McKinney 2007). See also 31 U.S.C. § 3729 (2011).

discretion of the government¹³⁰ and aggrieved parties cannot initiate the criminal claims. The government may initiate criminal claims in one of three ways: (1) an indictment voted by a grand jury; (2) the filing of “an information” by a prosecuting district or state’s attorney alleging that the crime was committed; or (3) the filing of a criminal complaint, which petitions the district attorney to initiate the charges.¹³¹

District Attorneys can prosecute health care fraud under various sections of Title 18 of the United States Code.¹³² Health care fraud is defined under Title 18 as an act “to defraud any health care benefit program; or (2) to obtain, by means of false or fraudulent pretenses, representations, or promises, any of the money or property owned by, or under the custody or control of, any health care benefit program[.]”¹³³ Depending on the injury sustained as a result of the fraud, the law provides up to life imprisonment and significant fines of \$250,000 for an individual or \$500,000 for organizations.¹³⁴ One of the difficulties in pursuing this remedy is that the government must prove each element of the crime beyond a reasonable doubt.¹³⁵ The statute also requires the government to initiate the action, although the statute allows the aggrieved party to request the government to initiate it.¹³⁶

Both the Department of Justice (“DOJ”) and the Department of Health and Human Services (“HHS”) have cited limited funding as a significant problem in pursuing health insurance fraud.¹³⁷ Traditionally, limited funding has hampered the investigation and prosecution of health care fraud, but the issue regarding funding has

¹³⁰ *How Courts Work*, AM. BAR ASS’N, http://www.americanbar.org/groups/public_education/resources/law_related_education_network/how_courts_work/bringingcharge.html (last visited Feb. 10, 2017).

¹³¹ *Id.*

¹³² 18 U.S.C. § 1347(a) (2010).

¹³³ *Id.*

¹³⁴ *Id.*; *Appeals of Healthcare and Medicare Fraud Convictions*, THE L. OFFICE OF C.F. COWAN, PLLC, <https://www.federalcriminalappeal.lawyer/federal-appeals-of-health-care-fraud-and-medicare-fraud-convicti.html> (last visited Jul. 8, 2016).

¹³⁵ 18 U.S.C. § 1347 (2010); *United States v. Javan*, 383 Fed. Appx. 596, 599 (9th Cir. 2010) (“The Government presented evidence sufficient for a rational juror to find beyond a reasonable doubt that Javan ‘knowingly and willfully’ intended to defraud health insurers . . .”).

¹³⁶ 18 U.S.C. § 1347 (2010).

¹³⁷ Janet Shikles, *Health Insurance More Resources Needed to Combat Fraud and Abuse*, UNITED STATES GENERAL ACCOUNTING OFFICE (July 28, 1992), <http://www.gao.gov/assets/110/104703.pdf>.

changed in recent times.¹³⁸ The Affordable Care Act (“ACA”) has increased funding for anti-fraud investigations.¹³⁹ In 2007, the federal government created Medicare Fraud Strike Forces,¹⁴⁰ a joint program between the DOJ and HHS, in which DOJ prosecutors collaborate with agents from HHS’s Office of Inspector General to investigate allegations of fraud to allow Centers for Medicare & Medicaid Services (“CMS”) to suspend payments to providers suspected of committing fraud.¹⁴¹ However, only 10 out of the 94 judicial districts are designated as Strike Force Districts, and these are too few.¹⁴² These judicial districts each see an average of only 42 people a year charged with health care fraud.¹⁴³ Comparatively, in 2014, CMS had found that over 17,000 providers committed fraud.¹⁴⁴

B. Civil Penalties

Civil penalties are also available against “authorized users” committing health care fraud. Civil penalties exist under the Federal False Claims Act,¹⁴⁵ the New York False Claims Act State Finance Law,¹⁴⁶ and New York Consolidated Laws Social Services Law.¹⁴⁷ The aggrieved party may initiate civil penalties under the aforementioned statutes.¹⁴⁸ However, such penalties may be too expensive or burdensome to realize because the damages from the

¹³⁸ *U.S. Attorney Ramping Up Health Care Enforcement in Western Penn.*, COALITION AGAINST INSURANCE FRAUD (Sept. 27, 2015), <http://www.insurancefraud.org/IFNS-detail.htm?key=21046>.

¹³⁹ *Id.*; Patient Protection and Affordable Care Act, 42 U.S.C. § 18001 (2010).

¹⁴⁰ Informational Brochure, U.S. Dep’t of Health & Human Services: Office of the Inspector General, Medicare Fraud Strike Force, <http://oig.hhs.gov/fraud/strike-force/> (last updated June 30, 2016).

¹⁴¹ *Id.*

¹⁴² *Id.*; Informational Brochure, United States Courts, Court Role and Structure, <http://www.uscourts.gov/about-federal-courts/court-role-and-structure> (last visited Aug. 5, 2016).

¹⁴³ *U.S. Attorney Ramping Up Health Care Enforcement in Western Penn.*, COALITION AGAINST INSURANCE FRAUD, <http://www.insurancefraud.org/IFNS-detail.htm?key=21046> (last visited Nov. 26, 2015).

¹⁴⁴ *The \$272 billion swindle*, THE ECONOMIST (May 31, 2014), <http://www.economist.com/news/united-states/21603078-why-thieves-love-americas-health-care-system-272-billion-swindle>. “Since tighter screening was introduced under Obamacare, the CMS has stripped 17,000 providers of their licence to bill Medicare.” *Id.*

¹⁴⁵ 31 U.S.C. § 3729 (2009).

¹⁴⁶ N.Y. STATE FIN. LAW §§ 187-194 (McKinney 2013).

¹⁴⁷ N.Y. SOC. SERV. LAW § 145-b (McKinney 2007).

¹⁴⁸ *Id.*

individual incidents of fraud would be very small, and litigation costs are relatively high.¹⁴⁹ Additionally, a victim of fraud can seek damages as well as restitution by filing a fraud claim in state court.¹⁵⁰

The Federal False Claims Act¹⁵¹ is a federal statute that imposes liability on those who defraud government programs.¹⁵² Specifically, the act provides for a civil penalty between \$5,000 and \$10,000 “plus 3 times the amount in damages which the Government sustains because of the act of that person.”¹⁵³ The False Claims Act has a whistle blower provision, referred to as *qui tam relator*,¹⁵⁴ which allows people not affiliated with the government to file an action on behalf of the government.¹⁵⁵ The provision rewards the whistleblower, or relator, with a percentage of the money that the government recovers because of the *qui tam* lawsuit.¹⁵⁶ Persons filing under the act can receive between 10% and 30% of any recovered damages.¹⁵⁷ The statute also provides for the recovery of costs of litigation by the U.S. Government.¹⁵⁸ This statute has a 6-year statute of limitations.¹⁵⁹

New York law imposes civil penalties against those committing fraud as well. The New York False Claims Act holds liable individuals that file false claims for payment from any state or local government.¹⁶⁰ First, under the New York False Claims Act, the New York Attorney General, an individual, or a local government may file a lawsuit against a person that obtains funds from the state or local government through fraudulent conduct.¹⁶¹ Fraudulent conduct includes knowingly making false statements or false records

¹⁴⁹ *By The Numbers: Fraud Statistics*, COALITION AGAINST INSURANCE FRAUD, <http://www.insurancefraud.org/statistics.htm#Vlpkc4S0HOw> (last visited Feb. 10, 2017). “Health care organizations recorded an average cost of \$398 per breached record . . .” *Id.*

¹⁵⁰ Informational Brochure, U.S. Attorney’s Office N.D. of Ga, Understanding Restitution, <https://www.justice.gov/usao-ndga/victim-witness-assistance/understanding-restitution> (last updated Apr. 17, 2015).

¹⁵¹ 31 U.S.C. §§ 3729-3733 (2011).

¹⁵² 31 U.S.C. § 3729 (2011).

¹⁵³ *Id.*

¹⁵⁴ 31 U.S.C. § 3730 (2011).

¹⁵⁵ *Id.*

¹⁵⁶ *Id.*

¹⁵⁷ *Id.*

¹⁵⁸ *Id.*

¹⁵⁹ 31 U.S.C. § 3731 (2011).

¹⁶⁰ N.Y. STATE FIN. LAW § 189 (McKinney 2013).

¹⁶¹ N.Y. STATE FIN. LAW § 190 (McKinney 2013).

to obtain payments for a claim from the government.¹⁶² The New York False Claims Act makes liable anyone who:

- (a) knowingly presents, or causes to be presented a false or fraudulent claim for payment or approval;
- (b) knowingly makes, uses, or causes to be made or used, a false record or statement material to a false or fraudulent claim;¹⁶³

Like the federal statute, the New York False Claims Act includes a *qui tam* provision, which allows a whistle blower to receive between 15% and 30% of the amount recovered.¹⁶⁴ The penalty under this statute is between \$6,000 and \$12,000 per claim, and the perpetrator may be responsible for the government's legal fees.¹⁶⁵ The statute of limitations is 10 years, which is longer than the federal statute's 6-year statute of limitations.¹⁶⁶ Additionally, New York Consolidated Laws Social Services Law section 145-b creates civil penalties for false claims.¹⁶⁷ This statute defines a false statement as "a claim for payment made to the state . . . or an entity performing services under contract to the state . . . which serves as the basis for a claim or a rate of payment . . . [for] *health care* services."¹⁶⁸ Section 145-b allows for the recovery of treble damages as well as monetary penalties that can be as high as \$30,000 per claim for repeat violations.¹⁶⁹

A defrauded health insurer may also commence a lawsuit in state court seeking damages for fraud from the individual service providers who committed the fraud. Damages for fraud include nominal damages, which are awarded when the party has not suffered substantial loss and are often a small monetary sum,¹⁷⁰ and punitive damages, which are intended to punish the defendant.¹⁷¹ In either case, pursuing many individual service providers is likely to incur

¹⁶² N.Y. STATE FIN. LAW § 189 (McKinney 2013).

¹⁶³ *Id.*

¹⁶⁴ N.Y. STATE FIN. LAW § 190 (McKinney 2013).

¹⁶⁵ N.Y. STATE FIN. LAW § 189 (McKinney 2013).

¹⁶⁶ N.Y. STATE FIN. LAW § 192 (McKinney 2010).

¹⁶⁷ N.Y. SOC. SERV. LAW § 145-b (McKinney 2007).

¹⁶⁸ *Id.*

¹⁶⁹ *Id.*

¹⁷⁰ *Nappe v. Anschelwitz, Barr, Ansell & Bonello*, 97 N.J. 37, 48 (N.J. Sup. Ct. 1984) (stating "[t]he three basic types of legal damages are compensatory, nominal, and punitive").

¹⁷¹ *Id.*

considerable litigation expenses.¹⁷² It is costly for health insurance companies to litigate lawsuits against numerous service providers who cause relatively small amounts of economic injury, as compared with the much lower cost of litigating a lawsuit against one large defendant, such as National Union.¹⁷³

Health insurers that suffer losses from computer systems fraud only have these remedies available to them, and most of these remedies are either too difficult or not cost-effective to pursue. The criminal penalties require government cooperation, and civil penalties require expensive litigation against numerous service providers. For these reasons, health insurers are left with no good options.¹⁷⁴

V. PRELIMINARY RECOMMENDATIONS

This section will discuss how electronic records facilitate the commission of health care computer systems fraud, as well as make some preliminary recommendations for health insurers to avoid losses due to fraud, such as providing insurance coverage to health insurers for fraud committed specifically by authorized users. Because of the difficulties that a health insurer faces in pursuing litigation against the individual committing the fraud, and the ease with which fraud may be accomplished, the need for health insurance companies like Universal to properly insure themselves becomes paramount. The following three features of electronic health care records (“EHRs”) increase the ease with which health care fraud is accomplished: (1) the mandated use and proliferation of EHRs; (2) the electronic nature of EHRs; and (3) the complexity of electronic datasets, termed “big data.” The mandated use and proliferation of EHRs make it easier to commit fraud than with paper health care records. The electronic nature of EHRs creates an inherent susceptibility to manipulation that could make fraud more difficult to detect using current technology because of the size and complexity of the datasets.¹⁷⁵ This section will discuss how health care providers

¹⁷² Paula Hannaford-Agor & Nicole Waters, *Estimating the Cost of Civil Litigation*, NATIONAL CENTER FOR STATE COURTS (Jan. 2013), http://www.courtstatistics.org/~media/microsites/files/csp/data%20pdf/csph_online2.ashx.

¹⁷³ *Universal*, 37 N.E.3d 78.

¹⁷⁴ Other than negotiating better contract provisions. *See infra* section VI.

¹⁷⁵ *Manipulation of 12,000 Medical Records Made Easy by EHR*, HEALTH CARE RENEWAL BLOG (July 7, 2012), <http://hcrenewal.blogspot.com/2012/07/manipulation-of-12000-medical-records.html>. “This is another area where electronic records make possible tasks

should ensure that their computer fraud indemnification riders protect them against losses incurred by “authorized users” utilizing their access to the system to commit insurance fraud.

The recent proliferation of electronic health care records (“EHRs”)¹⁷⁶ is partially driven by mandates in the ACA,¹⁷⁷ which is designed to promote the “meaningful use” of electronic health care records, and the American Recovery and Reinvestment Act of 2009 (ARRA), which is designed to increase federal funding for health care technology.¹⁷⁸ “Meaningful use” is a program for Medicare that seeks to increase EHR usage by having health care providers show that they are using certified EHR technology.¹⁷⁹ The ACA mandates an increase in the number of hospitals and doctors that utilize EHRs.¹⁸⁰ Moreover, “meaningful use” sets objectives that health care providers must achieve in order to qualify for CMS financial incentive programs created by the ARRA.¹⁸¹

There are three stages of “meaningful use” objectives of the ACA, the first of which started in 2011, and the last of which is scheduled to end in 2018.¹⁸² In Stage 1, the objective is data capture and sharing.¹⁸³ This means eligible providers received funding to improve their electronic data capture and sharing of medical records.¹⁸⁴ This includes electronically capturing health care information, utilizing the captured health care information to track

that are probably impossible with paper. Altering 11,000+ records would be hard in paper charts, as the alterations would likely stick out in a pronounced manner.” *Id.*

¹⁷⁶ Informational Brochure, Centers for Medicare & Medicaid Services, *Electronic Health Records (EHR) Incentive Programs*, https://www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/index.html?redirect=/EHRIncentivePrograms/01_Overview.asp (last visited Feb. 10, 2016) [hereinafter “*Electronic Health Records*”].

¹⁷⁷ 42 U.S.C. § 18001 (2010).

¹⁷⁸ *Electronic Health Records*, *supra* note 179.

¹⁷⁹ *What is Meaningful Use*, HEALTH RESOURCES AND SERVICES ADMINISTRATION, <https://www.hrsa.gov/healthit/meaningfuluse/MU%20Stage1%20CQM/mu.html#> (last visited Apr. 27, 2016) (“Simply put, ‘meaningful use’ means providers need to show they’re using certified EHR technology in ways that can be measured significantly in quality and in quantity.”).

¹⁸⁰ 42 U.S.C. § 3007 (2010).

¹⁸¹ Informational Brochure, HealthIT, *Meaningful Use Definition & Objectives*, <https://www.healthit.gov/providers-professionals/meaningful-use-definition-objectives> (last updated Feb. 6, 2015) [hereinafter “*HealthIT*”].

¹⁸² *Id.*; *Electronic Health Records*, *supra* note 179.

¹⁸³ *HealthIT*, *supra* note 184.

¹⁸⁴ Informational Brochure, Aetna Health, *Meaningful Use Knowledge Hub*, <http://www.athenahealth.com/knowledge-hub/meaningful-use/stages> (last visited Feb. 10, 2017).

clinical conditions, and reporting of clinical quality measures and public health information.¹⁸⁵ The objective in Stage 2 is to utilize the EHRs for advanced clinical processes.¹⁸⁶ Health care providers will receive additional funding for extending their “EHR capabilities to a larger portion of their patient populations.”¹⁸⁷ The objective in Stage 3 is to utilize EHRs to improve patient outcomes.¹⁸⁸ To meet the objective of Stage 3, health care providers will have to use EHRs to improve the results of the medical care a patient receives.¹⁸⁹ To qualify for the CMS Medicaid EHR Incentive Program, the health care provider must “adopt, implement, upgrade or meaningfully use certified EHR technology”¹⁹⁰ The effect of these “meaningful use” objectives is that federal funding to health care providers to meet these objectives increases the use of EHRs. As will be discussed further below, this increase in EHRs means an increase in the ability of health care providers to commit fraud.

Since the passage of both the ACA and the ARRA, EHR utilization has seen predicted increases, which have translated into considerable “meaningful use” fraud.¹⁹¹ “Meaningful use” fraud occurs when health care providers receive federal funds under this program even though they are not actually complying with the “meaningful use” requirements but rather gaming the system.¹⁹² CMS’s financial incentives have provided an additional means for health care providers to commit fraud by utilizing EHRs. The CMS

¹⁸⁵ Informational Brochure, HealthIT, How to Attain Meaningful Use, <https://www.healthit.gov/providers-professionals/how-attain-meaningful-use> (last visited Mar. 5, 2017).

¹⁸⁶ HealthIT, *supra* note 184.

¹⁸⁷ HealthIT, *supra* note 184.

¹⁸⁸ HealthIT, *supra* note 184.

¹⁸⁹ HealthIT, *supra* note 184.

¹⁹⁰ Informational Brochure, CMS, Medicaid Electronic Health Record Incentive Payments for Eligible Professionals, CMS (May 2013), https://www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/Downloads/MLN_MedicaidEHRProgram_TipSheet_EP.pdf.

¹⁹¹ Mark Hagland, *Hospital Fined \$4.4 Million for Meaningful Use Fraud*, HEALTH CARE INFORMATICS, (May 4, 2015), <http://www.health-care-informatics.com/news-item/hospital-cfo-fined-44-million-meaningful-use-fraud> (“A former hospital CFO has been fined \$4.4 million for defrauding the federal government through the directing of staff to falsely attest to meaningful use under the HITECH (Health Information Technology for Economic and Clinical Health) Act.”).

¹⁹² Kyle Murphy, *Meaningful use fraud: HHS, DOJ Issue Warning*, EHR INTELLIGENCE (Sept. 25, 2012), <https://ehrintelligence.com/news/meaningful-use-fraud-hhs-doj-issue-warning/>.

Medicaid EHR Incentive Program is a “pay-and-chase” system.¹⁹³ A “pay-and-chase” system means that CMS pays a claim to health care providers, knowing that a third party is likely responsible for the claim and then attempts to recover the payment.¹⁹⁴ Health care providers can then submit fraudulent claims, and CMS may not seek recovery of the money.¹⁹⁵

The EHRs’ electronic nature makes fraudulent entry relatively easy for service providers¹⁹⁶ because it allows authorized users to commit fraud without having to resort to traditional hacking, which involves the modification of computer code that is outside of the original programmer’s objective.¹⁹⁷ Moreover, EHR fraud is easier to disguise because the volume and the velocity of the data that an EHR may submit facilitate the capacity to commit fraud in a non-traditional manner.¹⁹⁸

Additionally, EHRs allow for easy “copy and paste” or “cloning” fraud,¹⁹⁹ which occurs when the health care provider duplicates clinical notes by electronically copying them from one account and pasting them into another.²⁰⁰ While this technique allows for quicker data entry, cloning makes it easy for health care providers to bill for work not performed by simply borrowing clinical notes from another patient’s record.²⁰¹ Also, a survey of all 864 hospitals that received subsidies for EHR systems as of March 2012 found that only 24% of hospitals have any sort of policy regulating

¹⁹³ Heather Caspi, *How Common is Meaningful Use Fraud*, HEALTH CARE DIVE (June 24, 2015), <http://www.healthcarediver.com/news/how-common-is-meaningful-use-fraud/401261>.

¹⁹⁴ Karen Fletcher, *Medicare Now Required to Check for Fraud Before Paying Claims*, CALIFORNIA HEALTH ADVOCATES (Oct. 2004), <http://blog.cahealthadvocates.org/2010/10/medicare-checks-for-fraud-before-paying/>.

¹⁹⁵ *Electronic Health Records*, *supra* note 179.

¹⁹⁶ Joe Carlson, *Feds Eye Crackdown on Cut-and-Paste EHR Fraud*, MODERN HEALTH CARE (Dec. 10, 2013), <http://www.modernhealthcare.com/article/20131210/NEWS/312109965>.

¹⁹⁷ *Easy Definition of Hacking*, CYBER LAWS, <http://cyber.laws.com/hacking> (last visited Aug. 5, 2016).

¹⁹⁸ Joe Carlson, *supra* note 199 (“‘Certain EHR documentation features, if . . . used inappropriately, can result in poor data quality or fraud,’ according a report from HHS’ Office of the Inspector General.”).

¹⁹⁹ Joe Carlson, *supra* note 199.

²⁰⁰ Robert Wayne & Alex Krouse, *EHRs: Upcoding, Overpayment and the False Claims Act – Understanding the Risks*, AM. BAR ASS’N HEALTH L. SEC. (Nov. 2014), http://www.americanbar.org/publications/aba_health_esource/2013-14/november/ehrs.html.

²⁰¹ Joe Carlson, *supra* note 199.

proper use of copy and paste.²⁰² The ability of health care providers to commit fraud increases with the lack of hospital policies that govern cloning, the ease at which the fraud goes undetected, and the ease of accomplishing cloning.²⁰³

Another possible source of fraud in EHRs occurs when service providers “upcode” or “upcharge.”²⁰⁴ Upcoding and upcharging occur when an insurance provider is charged for a more expensive service than what was provided,²⁰⁵ which can be done by changing the medical billing code or by simply fraudulently pasting the data from a more expensive test or procedure into a patient’s record.²⁰⁶ In 2012, the New York Times found that there was “a surge in Medicare spending on the most costly services” entered using EHRs.²⁰⁷ Moreover, a study by the Office of Inspector General, Department of Health and Human Services, found that neither CMS nor its contractors had adjusted their policies for detecting fraud to encompass the new threats brought by EHRs.²⁰⁸ In this study, the Inspector General found that very few of its contractors could properly detect “whether a provider had copied language or overdocumented in a medical record.”²⁰⁹

The proliferation of EHRs in the era of big data makes it easier for health care providers to commit health care fraud.²¹⁰ The term “big data” encompasses data sets that are so complex that traditional data processing applications are inadequate.²¹¹ The complexity of big data can create many challenges within security, analysis, or privacy.²¹² Specifically, security and analysis are problematic because even though modern computing infrastructure

²⁰² Joe Carlson, *supra* note 199.

²⁰³ Joe Carlson, *supra* note 199.

²⁰⁴ Reed Abelson & Julie Creswell, *Report Finds More Flaws in Digitizing Patient Files*, NEW YORK TIMES (Jan. 8, 2014), <http://www.nytimes.com/2014/01/08/business/report-finds-more-flaws-in-digitizing-patient-files.html>.

²⁰⁵ *Id.*

²⁰⁶ *Id.*

²⁰⁷ *Id.*

²⁰⁸ Daniel R. Levinson, *CMS and its Contractors Have Adopted Few Program Integrity Practices to Address Vulnerabilities in EHRs*, OFFICE OF INSPECTOR GENERAL (Jan. 2014), <http://oig.hhs.gov/oei/reports/oei-01-11-00571.pdf>.

²⁰⁹ *Id.*

²¹⁰ Reed Abelson & Julie Creswell, *supra* note 207.

²¹¹ Informational Brochure, Cloud Security Alliance, *Top Ten Big Data Security and Privacy Challenges* (Nov. 2012), http://www.isaca.org/Groups/Professional-English/big-data/GroupDocuments/Big_Data_Top_Ten_v1.pdf [hereinafter “*Top Ten*”].

²¹² *Id.*

allows for real-time anomaly detection, the volume and variety of the data streams may either lead to false positives or miss anomalies altogether.²¹³ Privacy is an issue because even though the large volume of data can be anonymized, those that intend on committing fraud easily identify the user that created the data or to which patient the data belongs.²¹⁴ The volume, velocity, and variety of the data likewise make processing the data extremely challenging. The volume of the data makes the process of detecting fraudulent data from authorized users difficult because of the large amount of computing power required to process this large amount of information.²¹⁵ According to *The Economist*, “[t]he amount of digital information increases tenfold every five years.”²¹⁶ The velocity,²¹⁷ or speed at which users enter the data, makes it difficult to detect fraudulent data even from “authorized users” because the data arrive too quickly and in such large volumes that the computer system is unable to utilize traditional methods of analysis to detect fraud.²¹⁸ The data’s variety also makes it hard to detect fraudulent data from authorized users, rendering older models for security obsolete.²¹⁹

Because Universal’s computerized system allowed for direct submission of claims to the system and the vast majority of claims are processed, approved, and paid automatically, the above “big data” paradigm applies.²²⁰ One does not need to be a high-tech hacker to commit health care insurance computer fraud; a mere “authorized user” can commit “fraudulent entry.”

Thus, to keep up with rapidly advancing technology, health care providers should ensure that their computer fraud indemnification riders specifically and unambiguously protect them against losses incurred by “authorized users” utilizing their access to the system to commit insurance fraud. To protect against lawsuits

²¹³ *Id.*

²¹⁴ *Id.*

²¹⁵ Kenneth Cukier, *Data, Data Everywhere*, *THE ECONOMIST* (Feb. 25, 2010), <http://www.economist.com/node/15557443>.

²¹⁶ *Id.*

²¹⁷ *Merriam-Webster*, *Velocity*, <http://www.merriam-webster.com/dictionary/velocity> (last visited Nov., 28, 2015).

²¹⁸ *Top Ten*, *supra* note 214 (“traditional security mechanisms, which are tailored to securing small-scale static (as opposed to streaming) data, are inadequate.”).

²¹⁹ Drew Robb, *Cyber Security’s Big Data Problem*, *E-SECURITY PLANET* (Dec. 3, 2014), <http://www.esecurityplanet.com/network-security/cyber-securitys-big-data-problem.html>.

²²⁰ *Universal*, 37 N.E.3d at 79.

similar to *Universal* and *Morgan Stanley*, health insurance providers seeking to indemnify themselves against losses incurred by authorized users should expressly include fraudulent claims by authorized users in the definition of computer fraud.

The insurance industry should offer insurance that provides coverage against losses due to authorized users submitting fraudulent claims. An insurance policy providing coverage against losses due to fraudulent entry by authorized users has a largely untapped market that could provide revenue for forward-thinking insurance companies.

VI. CONCLUSION

The current law governing indemnification for computer systems fraud does not benefit the insured. In *Universal*, the New York Court of Appeals found that a rider indemnifying the insured for losses from computer systems fraud covers only unauthorized use of the computer system and did not cover fraudulent use by an authorized user.²²¹ Hence, the court in *Universal* precluded coverage for losses incurred by an authorized user.²²²

This note's analysis of the various criteria for both fraudulent use and unauthorized users demonstrates that courts have discretion to find that similar provisions for insurance fraud could cover the insured in future cases. Additionally, the difficulty that health insurance companies face in seeking redress should cause the insured to carefully review the wording of their contracts; otherwise, they have no guarantee that they will be covered for this type of fraud.

As illustrated by both *Universal* and *Morgan Stanley*, both the New York Court of Appeals and the Superior Court of New Jersey Appellate Division have precluded coverage for losses incurred by an authorized user of the insured's computer system committing fraudulent acts.²²³ Health insurance companies seeking indemnification for these kinds of losses should seek additional advice as to whether their current Computer Systems Fraud rider

²²¹ *Universal*, 37 N.E.3d at 81. "[W]e conclude that it unambiguously applies to losses incurred from unauthorized access to Universal's computer system, and not to losses resulting from fraudulent content submitted to the computer system by authorized users." *Id.*

²²² *Id.*

²²³ See *Universal*, 37 N.E.3d 78; See also *Morgan Stanley*, 2005 WL 3242234.

offers the coverage they seek, and in the case that it does not, they should seek additional coverage.