Nature of Bankruptcy Work Changing Amid Filing Declines

By David Gialanella

Bankruptcy counseling—referred to by one attorney as “an industry in consolidation”—has always been a cyclical business, but the steady, years-long decline in new cases has required lawyers to rethink their practices to some extent.

“The drop-off that we’ve seen is in the midsize-to-smaller-size Chapter 11s,” said Stephen Packman, who chairs the bankruptcy, restructuring and insolvency litigation group at Haddonfield-based Archer & Greiner and practices in the firm’s Philadelphia office.

“There’s more out-of-court workouts; there’s more pre-packaged deals,” he added. “There’s been more bankruptcies that are either largely sales or liquidations.

“Certainly the work we would traditionally do in the region has downsized,” he said.

Lawyer’s ‘Puerile Name-Calling’ Helps Sink $2.5M Award

By Zack Needles

A plaintiffs lawyer’s persistent “inappropriate commentary” throughout a personal injury trial, including calling defense counsel’s questions during cross-examination “stupid,” required an award of more than $2.5 million to be overturned and the case to be retried, a New Jersey appeals court has ruled.

In an unpublished per curiam opinion

Universities ‘Peculiar Creatures’ in Cybersecurity World

By David Gialanella

Cyberattacks targeting Rutgers University and Penn State University have brought the issue of cybersecurity close to home—but also served to re-establish that higher-education institutions are unique targets.

“Universities are kind of peculiar creatures for cybersecurity,” said Vincent Polley, an attorney based near Detroit who co-authored “The ABA Cybersecurity Handbook” and who heads technology consultancy KnowConnect.

In the university structure—a confederation of schools that are fairly loosely coordinated”—there’s “frequently not a lot of top-down management,” he said.

NJ’s Definition Of ‘Employee’ Revives Sleepy’s Class Suit

By Charles Toutant

The U.S. Court of Appeals for the Third Circuit has reopened a putative class action against mattress retailer Sleepy’s in light of a January decision by the New Jersey Supreme Court that adopted a broad definition of who should be classified as an employee.

The appeals court vacated a district judge’s summary judgment order dismissing the case and remanded it for rehearing in light of the state Supreme Court’s adoption of what is known as the “ABC” test. The Third Circuit instructed the district court to apply the test to determine

Nature of Bankruptcy Work Changing Amid Filing Declines

Continued on page 10

Universities ‘Peculiar Creatures’ in Cybersecurity World

Continued on page 20

NJ’s Definition Of ‘Employee’ Revives Sleepy’s Class Suit

Continued on page 17
Universities ‘Peculiar Creatures’ in Cybersecurity World

Continued from page 1

What’s frustrating about the Rutgers attack that began in March—as well as another attack at nearby Fairleigh Dickinson University (FDU) around the same time—is that neither appears to be a nation-state or simple anger.

Both universities, according to reports, experienced what are called distributed denial-of-service (DDoS) attacks, which seek to deluge the target’s systems with requests that come from outside machines, said Polley, former co-chair of the information technology and security law practice group at Detroit-based Dickinson Wright.

DDoS attacks entail an orchestrator gaining control of those machines, sometimes through email “worms,” and then sending them to send protected information requests. The objective is that the target site or server, flooded with requests, is crippled and goes down.

Gideon Lenkey, president of Milford-based information security firm R2 Security Systems, said, “It’s hard to find because the requests that are attacking are not knowingly attacking.”

But Polley said a DDoS attack is not taking advantage of system vulnerabilities.

He called them “trivial attacks” and “nuisance attacks” that harness the “power to be disruptive,” and said how long an attack is offline depends on the sophistication of both the target and the orchestrator.

Both Polley and Lenkey said a DDoS attack can be motivated by personal politics or simple anger.

“It makes me think of a nation-state versus some kid in his basement just trying to cause damage,” said Lezza Garber, corporate counsel and director of business development at technology consultancy Capsicum Group in Philadelphia, which got its start as the technology arm of law firm Pepper Hamilton.

Attorneys said it may seem easier to gloss over if there wasn’t personal information taken, but “all of these varied types of cybercrimes are malicious—with different motives,” Garber said.

“When a DDoS attack may not seek direct financial gain, causing a network to fail can cause a host of other issues for a university in particular,” Garber said.

FDU’s attack was resolved fairly quickly, while Rutgers experienced multiple Internet outages—apparently the result of multiple attacks—that ended up affecting final exam schedules, according to reports.

Rutgers spokesman E.J. Miranda said the university—which found no evidence that confidential information was compromised during the incidents—has not retained outside counsel to advise on cybersecurity, but did retain outside vendors.

“Rutgers, like all academic, government and corporate institutions, is increasing the resources dedicated to protecting its information and continuously monitors our university data and electronic environments,” Miranda said in a statement.

“We resolved the DDoS issues and have implemented new safeguards and retained new cybersecurity vendors in the wake of the incidents,” he added.

Rutgers, as any institution with an Internet presence, continuously monitors our Web connections and servers to detect and respond to such issues as viruses, malware, denial of service and phishing. We have also retained a firm to assist in evaluating and developing security practices to control the management of sensitive data through various types and layers of security,” an FDU spokeswoman didn’t provide a comment by press time.

A spokesman from the U.S. Attorney’s Office said, “Our office is investigating Rutgers or FDU, though the FBI previously acknowledged its involvement, according to reports.

The nature of the Penn State issue—which was reported more recently, in May—appears to have been different.

The university said the College of Engineering’s network sustained two attacks last November, with at least one of those carried out by a hacker located in China.

In a May 15 statement that quoted numerous school officials, Kevin Moroney, Penn State vice provost for information technology, said, “Our information security protocols and practices help us to turn back millions of malicious computer attacks against the university every day.

“However, in this case we are dealing with the highest level of sophistication,” the statement said. “Unfortunately, we now live in an environment where no computer network can ever be completely, 100 percent secure.”

The university addressed the cyberattack privately, in order not to tip off the attackers, according to the statement.

The events at Rutgers, FDU and Penn State—all have large university clients, such as the University of Maryland—bear a common saying among cybersecurity experts: that it’s “not a matter of if, but when,” an attack will occur.

Cybersecurity lawyers interviewed last October warned of universities vulnerability, but maintaining defenses at a university or anywhere else is not so much a question of foresight as it is one of the practicality: Email-based attacks often rely on breaching a barrier that Lenkey previously referred to as “the human fire wall”—which is often the last but weakest line of defense, he said.

Christie at McCarter & English noted that universities provide a high number of network access points, for student convenience, and aren’t necessarily on the lookout for actions such as large data file transfers or multiple requests for access by a single user name, which would set off alarms for a nonuniversity client.

Another cybersecurity lawyer, Fernando Pinguelo, agreed that universities’ structures make them special cases.

It creates “a unique situation because, when you’re dealing with a company, you’re not integrating the clients into the IT systems,” said Pinguelo, who chairs Scarnici Hollenbeck’s cybersecurity and data protection group out of the firm’s Ocean office.

Universities in many ways are fundamentally different from retailers and other corporations, he pointed out, they all have budgets to heed.

“It’s like any organization, for-profit or otherwise,” Pinguelo said. “It can sometimes be the last issue to address. When it isn’t part of your money-making stream, I find that it often isn’t addressed as quickly or completely.

“The fact of the matter is, even if you spend every available resource trying to create this wall, there’s always going to be a way to break it.”

Contact the reporter at dgialanel-la@alm.com.

Obituary

Tompkins McGuire Founder William McGuire Dead at 86

William B. McGuire, founder of the Newark firm that eventually came to be known as Tompkins, McGuire, Wachenfeld & Barry, died May 13. He was 86.

A Seton Hall Law School graduate, McGuire worked as an assistant prosecutor in Essex County under then-Prosecutor Brendan T. Byrne and went on to become a senior partner at Lam, Faire & Foster. In 1984, he and other attorneys formed Tompkins, McGuire & Wachenfeld, which changed its name to Tompkins, McGuire, Wachenfeld & Barry in 1998. He focused his practice on complex insurance coverage, professional liability defense, directors and officers lawsuits, class actions, securities law, mercial litigation.

At various points in his career, McGuire served as president of the Essex County Bar Association, the New Jersey State Bar Association, the New Jersey State Bar Foundation and the Association of the Federal Bar of the District of New Jersey. He was also elected a fellow of the American College of Trial Lawyers in 1974 and served as vice president of the Trial Attorneys of New Jersey from 1978 to 1980.

McGuire received several awards over the years, including the Hon. William J. Brennan Jr. Award, given by the Association of the Federal Bar of New Jersey in 1997, and the first Thomas More Award, given to him by Seton Hall University in 1980. ■