GDB LAW

Winter 2018

LEGAL UPDATE

Providing current information about legal developments for our clients and friends.

Computer Security Laws Put Increased Pressure on Businesses to Adopt Stronger Cybersecurity Measures

Here Are Some Basic Steps You Should Take

By: Jay L. Hack, Esq.

Computer hacking, cybersecurity and selling social security numbers on the "Dark Web" are front page topics almost every day. Computer hackers are not just concerns of political parties, Equifax and Target. Does your company have customer personal data, like social security or driver's license numbers? Do you do business with any state-licensed company in the banking, insurance or mortgage lending business so that you have access to its computerized data?

If you answer "yes" to the first question, then you must tell your customers if your computer system is penetrated and their data may have been compromised. If you answer "yes" to the second question, then the bank, insurance company, mortgage lender or other related business may force you to choose between maintaining procedures designed to protect the data from wrongful intrusion or lose the ability to do business with it.

New York and almost every other state have security breach notification laws which generally require businesses to notify customers if a computer system has been breached and customer personal information has been accessed without authority.

In addition, New York's Department of Financial Services ("DFS") has recently adopted regulations that require banks, insurance companies, and other regulated financial services institutions to have vendor-management programs so that not only the regulated institution, but anyone else that it does business with, will have to adopt stringent cybersecurity programs to protect against intrusions. Even if you are not one of these regulated businesses, but rather you merely provide services to one of them, you can expect that you will have to adopt strict cybersecurity measures to satisfy their vendor management program. DFS may not be able to regulate you directly, but DFS can tell the banks and insurance licensees not to do business with you unless you implement cyber controls that protect any data you get from them.

Here are some steps we recommend to protect against running afoul of these laws:

- Adopt a formal information security plan that limits the amount of protected information that you maintain. If you manage a building, do you really need to keep an electronic copy of every tenant's driver's license on your computer? And if you do, think about blotting out the license number and the date of birth on the copy you keep. You can't be sued for wrongfully releasing data you don't have.

continues on page 6

New IRS Rules Govern Audits of Partnerships and LLCs Treated as Partnerships

You May Need to Revise Your Entity's Governing Documents

By: David N. Milner, Esq. & Asher Rubinstein, Esq.

Effective for partnership tax years beginning after December 31, 2017, the IRS has adopted new rules which apply to audits of income tax returns filed by partnerships, limited partnerships and limited liability companies treated as partnerships for tax purposes (all of which are referred to in this article as partnerships). These new audit rules are important because they have the potential to expose those who were not partners during the tax year being audited to the tax errors and liabilities of the partnership, which, under the prior rules, would have been the responsibility of those who were partners during the year under audit.

Under the old rules, if the IRS decides that taxable income had been incorrectly determined, the amount of the IRS adjustment would be allocated to each partner using that partner's profit sharing percentage for the year in question. The partner would then file an amended return (or the IRS would do so for him) and pay any additional income tax that may have been due (or receive a refund if the IRS' determination was that income had been underreported by the partnership).

continues on page 7

IN THIS ISSUE

NLRB Reverses Earlier Ruling Which Had Expanded Union Rights Against Franchisors and Other Contracting Companies

By: David T. Azrin, Esq.

In December 2017, the National Labor Relations Board (NLRB), which enforces federal union laws, reversed a 2015 ruling, called Browning-Ferris. The Browning-Ferris ruling, discussed in our Winter 2016 newsletter, had shaken up the franchise community by expanding the definition of a "joint employer" to the point where franchisors might be held liable for the labor law violations committed by their franchisees, even if the franchisor did not control the franchisee's employment decisions.

The December 2017 decision, called Hy-Brand Industrial Contractors, issued by a reconstituted board, reversed Browning-Ferris and reinstated the prior narrower "joint employer" legal test that had been applied for decades by the NLRB and the courts.

> *In most franchise arrangements, although the franchisor sets general standards for operation, the franchisor does not make the actual decisions regarding hiring and firing of employees, or setting their hours and wages.*

The "joint employer" test becomes important when a franchisee has allegedly committed labor law violations, and its employees try to hold both the franchisor as well as the franchisee liable, or a union representing a franchisee's employees tries to impose the obligation to engage in collective bargaining on both the franchisor and the franchisee.

Under the more narrow test, which had been in force for decades, the franchisor could only be held liable if it exercised actual control over the terms and conditions of the employees' employment, such as hiring, firing, and setting wages and hours, and the control was direct and not limited. In most franchise arrangements, although the franchisor sets general standards for operation, the franchisor does not make the actual decisions regarding hiring and firing of employees, or setting their hours and wages.

The earlier 2015 ruling had expanded the "joint employer" doctrine, holding that a franchisor could be held liable if the franchisor merely had the power or potential to

continues on page 6

GDB PARTNERS

DAVID T. AZRIN
dta@gdblaw.com
Franchise, Trademark, Employment, Litigation

DAVID L. BERKEY
dlb@gdblaw.com
Real Estate, Co-op/Condo, Litigation

MORRELL I. BERKOWITZ
mib@gdblaw.com
Litigation, Real Estate

MARK B. BRENNER
mbb@gdblaw.com
Corporate, Bankruptcy, Real Estate

DAVID S. DOUGLAS
dsd@gdblaw.com
Litigation

DAVID I. FAUST
dif@gdblaw.com
Corporate, Trusts and Estates, Tax, Real Estate, International Business Law

ADAM M. FELSENSTEIN
amf@gdblaw.com
Litigation, White Collar Criminal Defense

JAY L. HACK
jlh@gdblaw.com
Banking, Securities, Corporate

RANDY J. HELLER
rjh@gdblaw.com
Construction, Suretyship, Litigation

BEATRICE LESSER
bl@gdblaw.com
Real Estate Litigation, Co-op/Condo, Commercial and Residential Landlord/Tenant

MARC J. LUXEMBURG
mjl@gdblaw.com
Real Estate, Co-op/Condo, Corporate, Litigation

PETER R. MASSA
prm@gdblaw.com
Co-op/Condo, Real Estate, Corporate, Banking

DAVID N. MILNER
dnm@gdblaw.com
Tax, Trusts and Estates, Corporate, Real Estate

PERRY L. MINTZ
plm@gdblaw.com
Real Estate, Co-op/Condo, Corporate

SEYMOUR D. REICH
sdr@gdblaw.com
Trusts and Estates, Real Estate

ASHER RUBINSTEIN
ar@gdblaw.com
Asset Protection, Tax, Trusts and Estates

SCOTT M. SMILER
sms@gdblaw.com
Real Estate, Co-op/Condo, Corporate

ROGER L. STAVIS
rls@gdblaw.com
White Collar Criminal Defense, Investigations

JERRY A. WEISS
jaw@gdblaw.com
Real Estate, Co-op/Condo, Litigation

U.S. Supreme Court Expected to Issue Important Decision on Cell Phone Privacy Rights

By: Adam M. Felsenstein, Esq.

The U.S. Supreme Court is expected to issue a decision soon in a case which will have important ramifications for law enforcement. Specifically, the Court is being asked to decide whether the government has the right to track someone's location by obtaining location information from cell phone towers without a warrant.

The case, *United States v. Carpenter*, involves the use of cell phone tower location data to prove a suspect's whereabouts during the commission of a crime. The government used cell phone tower data at trial to place the suspects within a half mile to two miles of several stores that were robbed. The government then used call log data obtained from the phone company to show a flurry of communication around the time of the robbery. The defendants were ultimately convicted of robbery, and have taken an appeal. The U.S. Supreme Court is now wrestling with the question of whether the defendants had an expectation of privacy in the location data that was exchanged with the cell phone tower, and whether accessing that data without a warrant constituted an illegal search. A decision is expected before June 2018.

The Fourth Amendment protects people from the unreasonable search and seizure of their "houses, papers and effects," and requires the issuance of a search warrant before the Government may conduct any such search. Of course, the Fourth Amendment was drafted 218 years before the iPhone became available. Its drafters, even with all of their wisdom and foresight, did not contemplate a device that could constantly emit one's location to a third party. Now, the Supreme Court is faced with the question of how to handle such data during a criminal prosecution in light of the Fourth Amendment.

The government obtained the cell phone location records in the *United States v. Carpenter* case by making a record request under the 1986 federal law called the Stored Communications Act, which allows the government to obtain records from wireless providers by merely showing that the records were relevant to an investigation. To obtain the records with a warrant, the government would have been required to show that there was probable cause that a crime had been committed, which is more difficult.

> *The Fourth Amendment protects people from the unreasonable search and seizure of their "houses, papers and effects," and requires the issuance of a search warrant before the Government may conduct any such search.*

The defendant argued that the government violated his Fourth Amendment right to privacy by tracking his movements though his cell phone. The government argued that it did not need a warrant because the defendant gave up any expectation of privacy or property interest in the information when his cell phone gave the information to a third party, the wireless provider. Under the government's theory, the government is merely obtaining the information from a thirty party witness, and therefore, it does not need to get a warrant.

The U.S. Supreme Court has previously suggested that people may still have some expectation of privacy in information, even when it is shared with or stored by a third party.

In its 2012 decision in *United States v. Jones*, the U.S. Supreme Court held that the government could not attach a GPS tracking device to the underside of a suspect's car without first obtaining a warrant. The government argued that the suspect had no expectation of privacy in his whereabouts on public streets, and thus merely observing those whereabouts, even with technological assistance, did not violate the Fourth Amendment. The Court nevertheless found that attaching something to the underside of a car was an intrusion onto the suspect's property, rendering the search illegal. The Supreme Court left undecided the question of whether the Government could review GPS data emitted by a cell phone without the attachment of a device to one's car.

In 2014, the Supreme Court decided an issue regarding cell phone privacy in *Riley v. California*, namely whether a police officer may search a cell phone without a warrant, immediately following an arrest. Prior precedent provides that the police are allowed to conduct a limited search of a suspect following an arrest to ensure that the suspect is not dangerous, and to avoid the destruction of evidence. The Supreme Court held that searching a suspect's cell phone after an arrest, but without a warrant, was a step too far. The Court found the need for police officer safety and potential destruction of data was outweighed by the strictures of the Fourth Amendment. The Court however declined to answer the question of whether the police could intercept or observe data being emitted from the phone without a warrant.

In *U.S. v. Carpenter*, the Court is now being asked to answer this question directly. The decision may have important ramifications for law enforcement, because it may affect the surveillance practices of government agencies that rely on collecting this type of information. The decision is also expected to provide guidance on what type of information should be considered "private" in an era marked by rapid technological change.

ABOUT THE AUTHOR

Adam M. Felsenstein *is a partner at Gallet Dreyer & Berkey, LLP. His practice focuses on civil and criminal litigation matters, including trial work in state and federal courts. Mr. Felsenstein can be reached at amf@gdblaw.com.*

Corporate Officers Beware: You May Be Held Personally Liable for Fraud

By: Randy J. Heller, Esq.

The corporate form may shield an officer or director acting in his or her official capacity from personal liability in most settings, and it is usually hard to "pierce the corporate veil." Nevertheless, if such an individual commits a "tort" (which includes many types of fraud and misrepresentation), a corporate officer may be held personally liable.

It is commonly believed that forming a corporation shields individuals from personal liability for acts or omissions they commit in their official capacity as officers or directors of the corporation. That is often true. But a recent case by a New York appellate court reminds us of an important exception to that rule.

In *North Shore Architectural Stone, Inc. v. American Artisan Construction, Inc.*, a contractor (North Shore) sued a supplier (Artisan) in connection with a delivery of limestone to a project. The owner of the project contended that a recent delivery had missing pieces. At first, Artisan reported that the missing pieces had been stolen. As a result, North Shore agreed to pay Artisan for replacement pieces. But later it was alleged that Artisan had never supplied the missing pieces in the first place and had misrepresented what happened in order to obtain duplicate payment.

> *One who commits a tort (which includes fraud and misrepresentation) can be held individually liable regardless of whether he acted on behalf of the corporation or whether the corporate veil is pierced.*

North Shore sued Artisan as well as its president for conversion and fraud. The president moved to dismiss the claims against him on the grounds that he was at all times acting in his capacity as an officer of Artisan and not in his individual capacity. The lower court dismissed the claims against the president, stating that there was no basis to "pierce the corporate veil."

But the appellate court reinstated the claims. As it explained, since the complaint had alleged that the president "misrepresented the facts regarding the delivery of the original limestone, with the intent of inducing the plaintiff to rely on it," he could be personally liable whether or not he acted in his official duties as president. One who commits a tort (which includes fraud and misrepresentation) can be held individually liable regardless of whether he acted on behalf of the corporation or whether the corporate veil is pierced.

The case serves as a reminder to corporate officers that, in certain circumstances, they may be held personally liable for their actions if they commit fraud or other tortious conduct. The case also raises questions as to what other types of representations routinely made by corporate officers, such as promises made concerning payment of subcontractors and vendors, use of minority business enterprises, or financial solvency, might possibly form the basis of a fraud claim that could subject an executive to individual liability.

ABOUT THE AUTHOR

Randy J. Heller *is a partner at Gallet Dreyer & Berkey, LLP. He represents contractors and owners in a wide array of sophisticated construction-related matters as well as litigation. In addition to being named a Super Lawyer for many years running, as featured in The New York Times, Mr. Heller is considered one of the top attorneys in construction law in the New York metropolitan area by Best Lawyers of New York in The New York Times and The Wall Street Journal. In addition, Gallet Dreyer & Berkey, LLP has once again been given the highest "Tier 1" rating by U.S. News & World Report for its construction law practice. Mr. Heller can be reached at rjh@gdblaw.com.*

OUR PRACTICE AREAS INCLUDE:

- *Asset Protection*
- *Banking and Financial Institutions*
- *Bankruptcy*
- *Construction Law*
- *Co-op and Condo Law*
- *Corporate Finance and Securities*
- *Corporate Law*
- *Employment Law*
- *Franchising, Distribution and Licensing*
- *Intellectual Property*
- *International Business Law*
- *Litigation*
- *Mergers and Acquisitions*
- *Real Estate Law*
- *Tax Law*
- *Trusts and Estates*
- *White Collar Criminal Defense*

GDB ANNOUNCEMENTS

GDB is proud to announce that Adam M. Felsenstein has been promoted to partner

An experienced litigator and trial lawyer, Adam's practice focuses on commercial litigation and white collar defense. Adam has substantial trial experience in state and federal courts in a variety of complex business and criminal matters. Adam has been recognized by Super Lawyers as a New York Metro Rising Star for 2015, 2016 and 2017.

GDB welcomes Jared B. Foley as a new attorney

Jared B. Foley joined Gallet Dreyer & Berkey, LLP in December as counsel.

Jared's practice focuses on commercial litigation, white collar criminal defense, employment litigation and intellectual property litigation. He is a graduate of Columbia Law School and Dartmouth College. Jared has successfully represented individuals and businesses in federal court and state court and has also represented parties in FINRA, AAA, and JAMS arbitrations.

FIRM NEWS AND HONORS

Marc J. Luxemburg

In September, partner Marc J. Luxemburg presented a seminar titled "An Introduction to Coop Board Responsibilities" for new directors with co-presenter Gregory Carlson, President of the National Association of Housing Cooperatives.

In November, Mr. Luxemburg also presented two seminars at the Annual Conference of the Council of New York Cooperatives and Condominiums. The first was on current significant legal decisions of the year 2017, which focused on legal decisions that impacted the operations of cooperatives and condominiums and how to deal with the challenges they present; the second was entitled "Are Reports of the Demise of the Business Judgment Rule Premature." It examined recent cases concerning the application of the business judgment rule to actions of the boards of cooperatives and condominiums

David S. Douglas

In November, partner David S. Douglas was appointed a member of the Advisory Committee for the Hudson River Discovery Center at Cortlandt Waterfront Park.

In January, Mr. Douglas' article titled "New York City Shakes Up the Freelance Sector" was published in the winter edition of the New York Business Law Journal of the New York State Bar Association.

Asher Rubinstein

In November, Asher Rubinstein's article, "Bitcoin Surges in Value Again: Tax Consequences" was published in TaxNet Pro, a Thompson Reuters publication.

David T. Azrin

In December, partner David T. Azrin hosted a panel discussion on Franchising and Private Equity. The panel, moderated by Gary Occhiogrosso of Franchise Growth Solutions, included private equity professionals, Roger Lipton, Grant Marcks, and Oz Bengur, and franchise advisor Lisa Oak. The program was conducted as part of the International Franchise Association's Franchise Business Network.

Jay L. Hack

In December, partner Jay L. Hack was appointed a member of the Editorial Advisory Board of NYSBA's New York Business Law Journal.

In January, Mr. Hack presented a seminar on the Business Judgment Rule to the Annual Meeting of the Banking Law Committee of the New York State Bar Association.

Pamela Gallagher

In January, associate Pamela Gallagher's article titled "New Regulations Clarify NY's Upcoming Paid Family Leave Benefits Law" was published in the winter edition of the New York Business Law Journal of the New York State Bar Association."

Computer Security Laws

(continued from page 1)

- Perform a risk assessment of your business and know all possible intrusion risks. Some are obvious — like outside hackers trying to break through a computer firewall. Others may be less so — like having computers without strong password protections.
- Review your risk assessment with your in-house or outside information technology staff. Ask them to supplement the risk assessment with any items you may have missed, and then work with them to protect against identified risks.
- Arrange for a penetration test of your system. This is not hiring a hacker to break into your system, but it is a reasonable attempt to identify Internet intrusion points that could be exploited by a hacker. In many cases, shutting down an intrusion point is easy and painless.
- Train your employees to be alert and smart when using any electronic device. Make sure that everyone attends a training session and have them sign an attendance sheet. Senior executives should not be exempt. They may need the training even more than younger employees, because they may have even less familiarity with electronic systems than younger employees. Remember that training is not fool proof. It is a start, but vigilance must continue after the training class is over.

> *Repeat your risk assessment every year and every time you have a significant change in business or technology.*

- Consider instituting access limitations for electronic data. Does every employee really need to have access to every document on your system for every client? Does your document management system have the ability to limit access? If so, use it.
- The National Institute of Standards and Technology (NIST) has recently changed its recommendation regarding password changing and now recommends against periodic changes. I doubt that following this recommendation will withstand a strong cross examination from an attorney for an aggrieved person who was injured because someone was using the same password for 5 years and a hacker found it. You should consider what password protection policy best suits your firm – but make sure that yellow stickies with passwords on computer monitors are forbidden.
- Establish policies and procedures for portable devices such as laptops, cell phones, tablets, etc. Do the same for remote access from home computers. Make sure that you can disable access for any remote device that is lost or stolen.
- Review your employee termination procedures. Immediately cut off their access to data and materials, and change their passwords.
- Wash, rinse, repeat. Repeat your risk assessment every year and every time you have a significant change in business or technology. Train all new employees and refresh the training of existing employees annually.

ABOUT THE AUTHOR

Jay L. Hack *is a partner at Gallet Dreyer & Berkey, LLP and head of the firm's banking department. Mr. Hack is the past Chair of the Business Law Section of the New York State Bar Association. His practice focuses on providing a full range of legal services to banks and other financial institutions. Mr. Hack can be reached at jlh@gdblaw.com.*

NRLB Franchise Ruling Reversal

(continued from page 2)

exercise such control. The decision had caused an uproar in the franchisor community because it meant that franchisors could be held liable as a joint employer, even if they did not get directly involved in the franchisee's operation. As a result, some franchisors became more wary of providing advice or guidance to franchisees.

The NLRB had relied upon this expanded definition of a joint employer in 2015 to file numerous administrative complaints against McDonalds, alleging the franchisor could be held liable under the "joint employer" liability theory for the franchisees' alleged violation of their employees' right to engage in concerted group activity which might lead to the formation of a union. Those proceedings are still on-going.

The NLRB's recent decision narrowing the definition of a joint employer will significantly hamper the NLRB's efforts to continue with the legal proceedings against McDonalds, and will likely forestall any further efforts by the NLRB to take similar administrative action against other franchisors or contracting companies.

ABOUT THE AUTHOR

David T. Azrin *a partner at Gallet Dreyer & Berkey, LLP, represents a range of business clients and individuals on employment, trademark, and franchise law matters. Mr. Azrin is the organizer of the International Franchise Association's franchise business network program in the New York City area. He has been named by Super Lawyers magazine as one of the top attorneys in franchise and distribution law in the New York metropolitan area, and by the editorial board of Franchise Times magazine as one of the top franchise attorneys ("Legal Eagle") in the United States. Mr. Azrin can be reached at dta@gdblaw.com.*

New IRS Rules for Audits of Partnerships and LLCs

(continued from page 1)

The new rules provide that the additional tax will be determined at the partnership level by applying the highest corporate income tax rate for the year in which the adjustment is made (not the highest rate for the year under review.) The tax will be payable by the partnership, effectively reducing the amount of distributions that will be available to the partners for the year of the adjustment. There will be no impact on those who were partners during the year being audited who had the "benefit" of the adjustment who are no longer partners.

The new rules also require that the partnership designate a "partnership representative" who will have the sole authority to act on behalf of the partnership in an IRS proceeding. This includes the audit, the appeal and any tax or other court proceeding. In the past, while partnerships were required to designate a "tax matters partner," the IRS was required to notify each of the partners of the audit and to open an audit of each of the partners' income tax return. The other partners had the ability to participate in the audit.

There are ways that partnerships can avoid the new rules in whole or in part:

- Partnerships that are required to issue 100 or fewer Schedule K-1s whose partners consist entirely of individuals, estates of deceased partners, C corporations or S corporations (however, each of the shareholders of the S corporation must be a "qualified partner" and will be counted in determining the number of partners who are required to receive a Schedule K-1) can annually elect to "opt-out" of the new rules when the partnership files its partnership income tax return. The old rules will apply to partnerships that opt-out.
- Partnerships that do not opt-out can elect to "push-out" the adjustment to their partners. Partnerships that elect to do so must make the election within 45 days after the date of the notice of the final partnership adjustment. Partnerships making a "push-out" election must compute a "safe-harbor" income tax amount that the partner can elect to pay as opposed to including the adjustment on the partner's tax return and paying the tax calculated to be due.

> *The new rules require that the partnership designate a "partnership representative" who will have the sole authority to act on behalf of the partnership in an IRS proceeding.*

Partners of partnerships should consider the following:

- Amending the partnership's governing documents to require that:
  - The partnership "opt-out" if permitted, or in the alternative, the partnership will "push-out" any adjustments.
  - New partners be indemnified by the partnership and former partners against any negative tax consequences or cash flow that may result from audits or assessments of tax returns filed before they became partners.
- Conversion of the partnership into a corporation that elects to be taxed as an S-corporation.
- Selecting a "partnership representative" and agreeing upon a method of replacing the person so designated.

We would be pleased to review your existing partnership agreements and limited liability company operating agreements in order to respond to the new rules or counsel you as to the creation of these agreements in light of the new rules.

ABOUT THE AUTHORS

David N. Milner *is a partner at Gallet Dreyer & Berkey, LLP. Mr. Milner's practice focuses on tax law, estate planning, corporate law, and real estate. Mr. Milner, who is also a certified public accountant, helps clients structure transactions in a manner calculated to reduce adverse tax consequences, and helps families develop estate planning strategies. He frequently speaks to community groups and trade organizations on matters relating to estate planning. Mr. Milner can be reached at dnm@gdblaw.com.*

Asher Rubinstein, *a partner at Gallet Dreyer & Berkey, LLP, provides advice and guidance regarding asset protection, U.S. tax, estate planning, and tax controversies. He represents foreign and domestic clients. Mr. Rubinstein is the author of the blog, www.assetlawyer.com. He can be reached at ar@gdblaw.com.*

GDB LAW GALLET DREYER & BERKEY, LLP

845 THIRD AVENUE, 5TH FL
NEW YORK, NY 10022-6601
T: 212.935.3131 ▪ **F:** 212.935.4514
WWW.GDBLAW.COM ▪ INFO@GDBLAW.COM

GDB LAW
GALLET DREYER & BERKEY, LLP

845 Third Avenue, 5th Fl
New York, NY 10022-6601