Estate Planning and Probate Section CLE Program
Webinar
October 29, 2021

Welcome/Announcements and Introduction
David Gower, Estate Planning and Probate Law Section Chair

12:00 PM – 1:00 PM

Program
Death in the Digital Age-New Legal Issues for Estate Planning & Probate
Alan S. Wernick, Aronberg Goldgehn

See page 3 for speaker bio.

Life in the 21st century is lived both online and offline for many people. The digital life includes many personal and business potentially valuable assets including financial assets (bank accounts, insurance policies, investments, cryptocurrencies, digital collectibles, nonfungible tokens, etc.), business records, e-mails, texts, social media, personal and family photos, personal memoirs, etc. More often than not (assuming that the heirs and/or survivors are even aware they exist) these assets are inaccessible without appropriate access credentials – such as a user name and password, answers to secret questions, and/or biometric data, etc. – all of which may be lost if estate planning fails to appropriately and fully account for the digital life. If the individual is the owner of or key person in a business, poor planning – or no planning – of one's digital life could be fatal to the business. If the lawyer is holding the keys to his or her client's digital life, what happens if the lawyer is the victim of a cyberattack that compromises the confidentiality of the client's digital life, or the lawyer's confidential information (e.g., client files and/or business information)?

Link to Evaluation The evaluation must be completed to receive CLE credit.
https://www.surveymonkey.com/r/EstatePlanning10292021

Next Meeting: December 17, 2021 – Judges Panel with Judge Hayes and Judge Orel

DCBA Events:

November 11, 2021 – DCBA/D.A.W.L. Veterans Day CLE Program, Zoom

November 18, 2021 – DCBA Unwind – Reserve 22, Village Links of Glen Ellyn

December 8, 2021 – DCBA/DAWL/Justinian 2021 Grand Holiday Gala - Hotel Arista, Naperville

December 16, 201 – DBF Holiday Breakfast Fundraiser – Cooper's Corner, Winfield

Sign into Your Member Profile Before Registering for a CLE Program

Free CLE-credit is a major benefit of being a DCBA member. Beginning October 1, 2021, non DCBA members attending noon-time CLE will be able to receive credit when paying a $40 registration fee. It is important that DCBA members sign in on the DCBA website before registering for a CLE program, to avoid being charged the $40 fee. The newly updated DCBA website allows you to save your username and password, so signing in and registering for a CLE is easy to do. If you are not signed in, you will see a $40 to register. When logged in, you will see your registration is free as it always has been.

DCBA OnDemand CLE is Available on IICLE:

Members can find the link to The Illinois Institute for Continuing Legal Education (IICLE) catalog on the DCBA website under the menu item **CLE & Events→IICLE Online Library**. You must be logged into your DCBA Membership Profile to view courses for free or at a reduced price.

View & Print CLE Certificates through the DCBA Website:

Members can view and print their certificates for any DCBA CLE program attended by first signing into their account on the DCBA website. Hover over the **CLE & Events** menu item and select **Find My CLE Credits**. This page will list all the CLE credits earned with DCBA. To the left of each program is an icon to print or email the Statement of Credit. You can find certificates for all CLE credits earned in Illinois by signing into your account on the MCLE Board website.

ALAN S. WERNICK - Lawyer, Arbitrator/Mediator, and Writer. Alan is a Martindale AV-rated attorney and a Leading Lawyer in Computer and Technology Law, admitted to practice in IL, NY, OH, and DC. Alan helps clients in transactions and dispute resolution through his experience and a multidisciplinary background in law, technology, and accounting, in addition to his experience as an arbitrator/mediator. For more info visit his law firm bio: https://www.agdglaw.com/alan-s-wernick, his website: WWW.WERNICK.COM, or his LinkedIn profile: https://www.linkedin.com/in/alanwernick/.

A Publication of Law Bulletin Publishing Company
Chicago Lawyer®
Info Tech Law

Death and the digital age

April 2012

By Alan S. Wernick, Esq.
T: 847.786.1005 – E: Alan@Wernick.com

With an increasing amount of personal and business assets residing in digital form and accessible only through electronic means, you and your clients need to be mindful of what will happen to those digital assets when a person dies.

Digital assets include financial accounts, documents, e-mail, social media websites, music and photographs, to name a few. These digital assets may include some very personal and private items such as medical and financial information, personal notes to loved ones, personal diaries or writings about loved ones, photographs or drawings of loved ones, business plans, trade secrets and other items not meant, nor appropriate, for public disclosure.

Access to the digital assets most likely may require, at a minimum, knowledge of the user name and password (or, in some cases, possession of a working security token used in conjunction with the user name and password). However, when the digital assets are encrypted, knowledge of the encryption key will be necessary to unlock the encryption and see and read the digital assets.

For small- to medium-size businesses where there is one individual in control of the business and that individual dies, the digital assets of that individual and his or her business may be at risk of not being readily known or, if known, readily accessible. Those who may have an interest in the existence of the business' digital assets (e.g., family members, employees, creditors and claimants to intellectual property rights owned or used by the business) may not even be aware of the existence and location(s) of all of the digital assets. A business could fail if timely access to the digital assets of the business is not obtained.

Some states passed statutes or are considering legislation to provide executors of a deceased person's assets a right to take control of certain digital assets. Examples of such statutes include Connecticut (§45a-334a, Access to decedent's electronic mail account); Idaho (§15-3-715(28), Transactions authorized for personal representatives — exceptions); Indiana (§29-1-13-1.1, Duty of custodian to provide electronically stored documents to personal representative); Oklahoma (§269, Executor or administrator — powers); and Rhode Island (§33-27-1, Access to Decedents' Electronic Mail Accounts Act).

However, these state statutes are not uniform in their language and scope. For instance, the Oklahoma statute (§269) provides: "The executor or administrator of an estate shall have the power, where otherwise authorized, to take control of, conduct, continue or terminate any accounts of a deceased person on any social networking website, any microblogging or short message service website or any e-mail service websites." In contrast, the Connecticut statute (§45a-334a) only speaks to e-mail accounts.

In January, the Uniform Law Commission (nccusl.org) proposed a study committee to consider the drafting of uniform legislation concerning access to digital information by a fiduciary administering a decedent's estate. It will be a while before a proposed uniform statute, if any, is produced by the National Conference of Commissioners on Uniform State Laws and proposed for adoption.

Where the current, albeit limited, statutory resources available in this area fall short is in their approach to the contracts, licenses, intellectual property rights, privacy rights and the technologies that sit at the threshold to accessing many digital assets. Assuming that those who may have a legitimate need or desire to know about the digital assets of a decedent are even aware of the existence of the digital assets, how will they deal with the access and control of those assets?

Digital assets estate planning services have appeared on the Internet. These services offer a technology solution to handling digital assets. However, their terms of use are not all the same and may not present a comfortable legal risk model to individuals considering those services. Suffice it to say that before trusting the keys to one's digital life to a digital estate planning service, knowledgeable legal counsel should be consulted to review and discuss the terms of use with you.

Control over the digital assets may be stymied by the terms of use of the websites containing the digital assets. For instance, the social media website may not allow heirs to continue the decedent's social media presence as a memorial to the decedent. In some instances, the family or heirs may have valid reasons for wanting the decedent's social media presence to be promptly removed, but will have to work through the terms and conditions of the social media website provider.

What if the digital assets include a collection of e-books? Unlike traditional hardback or paperback books, which may be transferred pursuant to the first sale doctrine, e-books may be subject to license restrictions that prohibit or restrict copying or distribution. Since digital assets are (usually) very easy to copy, it may be an infringement of copyright rights if multiple copies of the digital asset are created and distributed to multiple heirs when the copyright rights are owned by a third party.

Like most things in life and in business, a little planning may go a long way in preserving and protecting one's digital legacy.

American Bar Association, Business Law Section, BLT Month-In-Brief: Internet Law & Cyber-Security – September, 2021

Biometric Information Privacy Act and Collective Bargaining Agreements

By Alan S. Wernick

In a September 20, 2021, decision, the U.S. Court of Appeals, 7th Circuit, held that a business that has entered into a Collective Bargaining Agreement ("CBA") governed by the Labor Management Relations Act ("LMRA") may look to the CBA to determine whether the union has consented on the employees' collective behalf regarding how the business (the employer) acquires and uses fingerprint (or other biometric) information of its employees subject to the CBA.

The plaintiffs in *Fernandez, et al., v Kerry, Inc.*, 2021 WL 4260667 (CA7, 20210920), were five persons who used to work for Kerry, Inc., in Illinois, and were seeking damages under the state's Biometric Information Privacy Act ("BIPA"), 740 ILCS 14/5 to 14/25. Among other things, BIPA requires private entities to obtain consent before collecting or using biometric information, including fingerprints. The lawsuit alleged, inter alia, that in 2011 Kerry began requiring workers to use their fingerprints to clock in and out of work. Initially filed in state court as a class action, the case was removed to federal court under 28 U.S.C. §1453, asserting that the class's total damages could exceed $5 million and that the statutory requirement of some diverse citizenship is satisfied. The U.S. District Court, in granting defendant's (Kerry's) motion to dismiss, held that §301 of the LMRA, 29 U.S.C. §185, preempts a state law claim if resolution of the claim "requires the interpretation of a collective-bargaining agreement."

The Court of Appeals stated, "After all, the statute [LMRA] says that a certified union is each worker's exclusive representative on collective issues. 29 U.S.C. § 159(a)." (Emphasis in the original.) Based on that premise, the Court concluded:

> Here, as in Miller [Miller v. Southwest Airlines Co., 926 F.3d 898, 903–05 (7th Cir. 2019)], the employer invokes a management-rights clause. We remarked in Miller: "Whether [the] unions did consent to the collection and use of biometric data, or perhaps grant authority through a management-rights clause, is a question for [decision under the agreement]. Similarly, the retention and destruction schedules for biometric data, and whether [employers] may use third parties to implement timekeeping and identification systems, are topics for bargaining between unions and management. States cannot bypass the mechanisms of [federal law] and authorize direct negotiation or litigation between workers and management." (emphasis in original). "It is not possible even in principle to litigate a dispute about how an [employer] acquires and uses fingerprint information for its whole workforce without asking whether the union has consented on the employees' collective behalf." We held in Miller that it was for an adjustment board—as here it is for an arbitrator—to decide whether the employer properly obtained the union's consent. (internal citations omitted)

The Court also noted that plaintiffs did not contend that Local 781 of the Miscellaneous Warehousemen, Airline, Automotive Parts, Service, Tire and Rental, Chemical and Petroleum, Ice, Paper, and Related Clerical and Production Employees Union choices violate its duty of fair representation, nor had they joined Local 781 as a defendant. The Court therefore affirmed the District Court's opinion that the plaintiffs' claims are preempted by §301 of the LMRA, 29 U.S.C. §185.

The bottom line is that employers who have a unionized workforce, and who are using, or plan to use, biometric processes/devices in connection with their employees, should carefully review and analyze their CBAs to determine whether or not the CBA appropriately, in light of the applicable law, addresses the employer's biometric processes/devices impacting their employees.

American Bank Association, Business Law Section, Business Law Today – October 1, 2021

SEC Increasing Cyber Threat Enforcement: Charges Issuer with Failure to Maintain Proper Cybersecurity Controls and Procedures

By Alan S. Wernick

In a June 14, 2021, Settlement Order[1] (the "Order"), the Securities and Exchange Commission ("SEC") alleged certain cybersecurity disclosure controls failures at First American Financial Corporation ("FAFC").

Without admitting or denying the SEC's findings, FAFC agreed to (1) cease and desist from further violations of SEC Exchange Act Rule 13a-15(a); and (2) pay a $487,616 penalty. Rule 13a-15(a) mandates that every issuer of a security registered pursuant to Section 12 of the Exchange Act must maintain disclosure controls and procedures to ensure that information the issuer must disclose in reports it files or submits pursuant to the Exchange Act is recorded, processed, summarized, and reported within the time periods specified in the SEC's rules and forms. FAFC provides products and services in connection with residential and commercial real estate transactions, including title insurance and escrow services. In connection with that business, FAFC issues common stock registered with the SEC pursuant to 12(b) of the Exchange Act. Many months before this SEC action arose, FAFC's IT security personnel had identified a computer system vulnerability that they failed to remedy in accordance with the company's policies, and about which they failed to inform the company's senior management.

On May 24, 2019, a cybersecurity journalist notified FAFC that its "EaglePro" application for sharing document images related to title and escrow transactions had a cybersecurity vulnerability. The vulnerability exposed over 800 million title and escrow document images dating back to 2003. These images included Personal Identifiable Information ("PII") such as social security numbers and financial information. In response to this notification, FAFC issued the following statement to the journalist: "First American has learned of a design defect in an application that made possible unauthorized access to customer data. At First American, security, privacy and confidentiality are of the highest priority and we are committed to protecting our customers' information. The company took immediate action to address the situation and shut down external access to the application." The journalist quoted this statement verbatim in his cybersecurity blog report published on the evening of May 24, 2019.[2]

FAFC then furnished a Form 8-K to the SEC on May 28, 2019, attaching an additional press release stating, in part, that there was "[n]o preliminary indication of large-scale unauthorized access to customer information." The press release also stated: "First

[1] In re First American Financial Corporation, SEC Admin. Proceeding No. 3-20367 (SEC Order, June 14, 2021) – https://www.sec.gov/litigation/admin/2021/34-92176.pdf.

[2] "First American Financial Corp. Leaked Hundreds of Millions of Title Insurance Records" (KrebsOnSecurity Blog Post, May 24, 2019) – https://krebsonsecurity.com/2019/05/first-american-financial-corp-leaked-hundreds-of-millions-of-title-insurance-records/.

American Financial Corporation advises that it shut down external access to a production environment with a reported design defect that created the potential for unauthorized access to customer data."

The June 2021 SEC Order arose in part because FAFC's senior executives responsible for the press statement and Form 8-K were not apprised of certain information concerning the company's information security personnel's prior knowledge of a vulnerability associated with FAFC's EaglePro system before making those statements – information that would have been relevant to management's assessment of the company's disclosure response to the vulnerability and the magnitude of the resulting risk. In particular, FAFC's senior executives were not informed that the company's information security personnel had identified a vulnerability several months earlier in a January 2019 manual penetration test of the EaglePro application ("January 2019 Report"), or that the company had failed to remediate the vulnerability in accordance with its policies. As discussed in the Order, FAFC did not maintain disclosure controls and procedures designed to ensure that senior management had this relevant information about the January 2019 Report prior to issuing the company's disclosures about the vulnerability.

As evidenced by the FAFC Order, and several additional recent enforcement actions, the SEC is viewing cybersecurity threats to businesses subject to SEC rules as a growing business risk. One such enforcement action concerned Pearson plc, a London-based public company listed on the New York Stock Exchange (with Pearson's ordinary shares registered under Section 12(b) of the Exchange Act). In August 2021, Pearson agreed to pay $1 million to settle charges that it misled investors about a 2018 data breach involving the theft of millions of student records, including dates of births and email addresses, and lacked adequate disclosure controls and procedures.[3]

Other recent SEC enforcement actions include sanctions against eight firms in three actions filed August 30, 2021, "for failures in their cybersecurity policies and procedures that resulted in email account takeovers exposing the personal information of thousands of customers and clients at each firm." The eight firms, which have agreed to settle the charges, are: Cetera Advisor Networks LLC, Cetera Investment Services LLC, Cetera Financial Specialists LLC, Cetera Advisors LLC, and Cetera Investment Advisers LLC (collectively, the Cetera Entities) – $300,000 penalty; Cambridge Investment Research Inc. and Cambridge Investment Research Advisors Inc. (collectively, Cambridge) – $250,000 penalty; and KMS Financial Services Inc. – $200,000 penalty. All were Commission-registered as broker dealers, investment advisory firms, or both. Kristina Littman, Chief of the SEC Enforcement Division's Cyber Unit, is quoted[4] as saying, "Investment advisers and broker dealers must fulfill their obligations concerning the protection of customer information…. It is not enough to write a policy requiring enhanced security measures if

[3] "SEC Charges Pearson plc for Misleading Investors About Cyber Breach" (SEC Press Release, August 16, 2021) – https://www.sec.gov/news/press-release/2021-154.
[4] "SEC Announces Three Actions Charging Deficient Cybersecurity Procedures" (SEC Press Release, August 30, 2021) – https://www.sec.gov/news/press-release/2021-169.

those requirements are not implemented or are only partially implemented, especially in the face of known attacks."

Collectively, these SEC enforcement actions underscore the importance of a business:

1. Having appropriate privacy and cybersecurity policies;
2. Educating/training employees about these policies;
3. Ensuring the business's contracting practices contain appropriate provisions consistent with these policies; and
4. Conducting periodic legal audits for compliance to these policies.

The FAFC Order also highlights the importance of executives maintaining an awareness of all material internal and external communications of the privacy and cybersecurity threats facing the business, and providing leadership from the top as to the importance of privacy and cybersecurity issues to the business's risk management.

Leadership and Cybersecurity

By Alan S. Wernick, Esq.

Will Rogers is quoted as saying: "People's minds are changed through observation and not through argument."[1] Business leaders do make a difference when it comes to data breaches and cybersecurity threats – which are almost a daily news item. Losses due to a data breach are expensive, particularly in a reactive (versus proactive) mode, and may include loss of trade secrets and other intellectual property assets; personal identifiable information ("PII") – credit card, financial, and medical data of customers, employees, and/or suppliers; loss of business goodwill; and loss of other valuable business assets. Empirical data, statutes/regulations, and developing case law underscore the compelling need for business leaders to proactively understand, identify, and manage cybersecurity legal and technology risks.

There have been several recent studies indicating the power of C-Suite's[2] leadership impact on a business' cybersecurity risks. A May 2016 study by the Ponemon Institute[3] titled "Tone at the Top and Third Party Risk" provides several interesting insights into business leadership and cybersecurity including:

- "Most C-level executives are not engaged in their organization's third party risk management process. Only 37 percent of respondents agree that the C-level executives in their organization believe they are ultimately accountable for the effectiveness of third party risk management. As a possible consequence of this lack of engagement, 50 percent of respondents do not believe the risk management process is aligned with business goals, which are most likely determined by senior management."
- "The CEO is expected to set a positive tone. Forty-one percent of respondents say it should be the CEO who sets the tone at the top, followed by 19 percent of respondent who say it is the compliance officer. Only 6 percent of respondents say the C-suite is most responsible for setting a positive tone at the top for the entire organization."
- "The consequences of not managing third party risk can be costly. In the past 12 months, organizations represented in this research spent an average of approximately $10 million to respond to a security incident as a result of negligent or malicious third parties."
- "Most C-level executives are not engaged in their organization's third party risk management process. Only 37 percent of respondents agree that the C-level executives in their organization

[1] Anyone who is a parent may have discovered this to be true….
[2] E.g., "CEO" – Chief Executive Officer; "CFO" – Chief Financial Officer; "COO" – Chief Operating Officer; "CIO" – Chief Information Officer.
[3] The Ponemon Institute (www.ponemon.org) conducts independent research on privacy, data protection and information security policy. Alan is one of several Ponemon Institute Fellows.

believe they are ultimately accountable for the effectiveness of third party risk management. As a possible consequence of this lack of engagement, 50 percent of respondents do not believe the risk management process is aligned with business goals, which are most likely determined by senior management."

- "Boards of directors are not actively engaged in risk management activities. Similar to the perceived lack of accountability on the part of C-suite executives, only 40 percent of respondents say their boards of directors are significantly involved (17 percent) or have at least some involvement in overseeing risk management activities (23 percent)."

So what, if anything, can the C-Suite and the Board of Directors do about cybersecurity threats to their business? "It depends" is probably the best answer. Members of the Board of Directors may not be required to have a detailed understanding of the applicable technologies, and may be able to rely, in part, on outside experts in evaluating and managing cybersecurity risks. When an active cyber threat is discovered (e.g., a data breach), their actions pre and post breach may be subject to review in any resulting litigation under the applicable law of the business judgment rule to determine if they followed the appropriate standards of care, loyalty, and good faith. Most likely, that analysis will depend on whether the actions (or inactions) taken by the C-Suite and the Board of Directors were reasonable and reflected good common sense in comparison to their peers in their industry.

There are a number of variables in play for cybersecurity risks for each business, including the industry, the applicable industry regulations and standards, the available skill set (e.g., does the CEO or CFO also have to function as the CIO and/or CPO for the business, or does the business have individuals with the appropriate experience in those roles; do the CEO and CFO have a technology background and/or experience), and the available resources for proactive versus reactive costs related to cybersecurity incidences, among other factors. The following, while by no means an exhaustive list, provides ten (10) initial items for consideration:

1. What assets are at risk? Examples include trade secrets and other intellectual property assets; personal identifiable information ("PII") – credit card, financial, and medical data of customers, employees, and/or suppliers; business goodwill; and other valuable intangible business assets.
2. Where are the assets stored? For example, are they stored in "the cloud," on a computer server with no connection to the Internet, in the United States or elsewhere?
3. Who has access to the assets? For example, what is the authorization/access protocols and hierarchy for each asset and how often is it verified and updated (e.g., does an employee departure automatically trigger an update to the authorization)?
4. What assets are encrypted and are they encrypted at all times (e.g., including in transit within and outside the business)?
5. When does the business do penetration testing to test for vulnerabilities?
6. What type of insurance coverage for cybersecurity risks of the business is in place and is it adequate for the cybersecurity risks confronting the business?

7. What types of physical (e.g., the secure and locked door) security and technology (e.g., firewalls, software monitoring tools, etc.) security are used for all of the assets?
8. How familiar are the C-Suite and the members of the board of directors (and members of committees of the BOD) with cybersecurity risks and compliance? What is their level of understanding of the different types of cybersecurity risks and the types of harm they may cause a business? Are they familiar with their industry standards concerning cybersecurity risks (for example, the NIST Cybersecurity Framework)? How will their actions (or inactions) be viewed in light of the applicable law of the business judgment rule if the board's failure to manage cybersecurity risks rises to the level of a breach of fiduciary duty?
9. What employee training programs, if any, are conducted by the business? And, what are the frequency and effectiveness of the training? Recent studies have shown that insider threats continue to pose increasingly significant privacy and cybersecurity problems for businesses. Sometimes that threat is from the intentional actions of a disgruntled employee, and sometimes the threat arises because of the uninformed employee (e.g., "I thought that e-mail asking me to transfer a million dollars to customer X's bank account was really from the CFO….").
10. When, if ever, did the business have a legal audit performed (e.g., a privacy audit or an intellectual property audit)? How frequent are these legal audits and are they being conducted by knowledgeable legal counsel?

While the above is not an exhaustive list, how comfortable are you with knowing the answers to these questions for your business? As the Chinese military general Sun Tzu said in "The Art of War:" "The art of war teaches us to rely not on the likelihood of the enemy's not coming, but on our own readiness to receive him; not on the chance of his not attacking, but rather on the fact that we have made our position unassailable."

The bottom line is cybersecurity risk correlates to whether or not the C-Suite and Board of Directors take the time to understand privacy and cybersecurity risks and embrace, educate, and manage as leaders in cybersecurity risk mitigation strategies appropriate to their business.

For comments about this article or to be added to the *ITIP Alert™* subscriber's list, please contact ALAN WERNICK (E-MAIL: ALAN@WERNICK.COM; PHONE: 847.786.1005 OR 614.463.1400).