INTELLECTUAL PROPERTY LAW COMMITTEE
BUSINESS LAW SECTION
THE FLORIDA BAR

MEETING MINUTES – FLORIDA BAR CONVENTION
Gaylord Palms, Orlando, FL – June 26, 2014

Ury Fischer, Chair, Coral Gables	ufischer@lfiplaw.com	305-448-7089
Dineen Wasylik, Legislative Vice Chair, Tampa	dineen@ip-appeals.com	813-778-5161
Woody Pollack, CLE Vice Chair, Tampa	woodrow.pollack@gray-robinson.com	813-273-5000
Jaime Vining, Social Media Vice Chair, Miami	rjv@friedlandvining.com	305-777-1720

Attendees: , Michael Chesal, Don Conwell, Dough Cherry, Ava Doppelt, Alejandro Fernandez, Jeffrey Feldman, Jim Gale, Brian Gilchrist, Matthew Horowitz, Allison Imber, Robert Kain , Keith Kanouse, Larry Kunin, Samuel Lewis, Jeff Lloyd, Kimra Major-Morris, Robert Norway, Steven Peretz, Woody Pollack, Joel Rothman, Darren Spielman, Mark Stein, , Kelly Stewart, Robert Thornburg, Jeanne Seewald, Dineen Wasylik, A. Robert Weaver, and Daniel Whitehouse.

I. WELCOME AND INTRODUCTION BY THE CHAIR

Chair Ury Fischer welcomed the group. Attendees each introduced themselves.

II. OLD BUSINESS

A. Adoption of Meeting Minutes. 5th Annual IP Symposium Meeting
The minutes that had been previously distributed by email were approved by voice acclimation.

B. Legislative Update

(1) Employee-Hacker Subcommittee – Robert Kain, Fort Lauderdale
Some history and issues related to the proposed Computer Abuse and Data Recovery Act (CADRA) were discussed. Previously issues dealt with how to define "without authority" in computer crimes. Various surveys exist relating to what is with and what is without authority. The first draft of CADRA had passed the IP Committee, but received some objections in the Business Litigation Committee, namely that the proposed legislation was too broad and had a multi-factored test for determining what was "without authority." There was concern, driven largely by judges in the Business Litigation Committee, that the issues would be brought

up in every CADRA case. At the Business Law Section retreat, a small committee was formed with 2-3 business litigation committee members, Ury Fischer, Sam Lewis, and Russ Landy (chair of the Business Litigation Committee) to address these concerns.

If you have a password controlled computer that is used in business, and someone steals a password or traffics in the password, then that is intended to be a CADRA violation. DMCA has some case law regarding "technological access barrier" and the small committee has adopted "technological access barrier" instead of password, as "technological access barrier" is broader. Technological access barrier includes password, security code, token, access device, or similar measure. The small committee also agreed that the technological access barrier, if it is a password, must be an effective password (i.e. "1234" or "admin" were no good).

No action is required of the IP Committee currently. The plan is to bring CADRA up for consideration by the IP Committee at the retreat.

(2) Proceedings Supplementary Task Force – Dineen Wasylik, Tampa
The taskforce is still working towards a more global solution and is hoping for proposed legislation by the retreat (to consider for the legislative session 2 years down the road).

(3) Covenants Not to Compete Task Force – Don Conwell, Tampa
Nothing to report and this Task Force is essentially defunct.

(4) New Legislative Issues – Dineen Wasylik, Tampa
The business identity theft statute did not pass this year. This is a priority of Rep. Passidomo. Its goal is to create criminal and civil penalties for taking the identity of a business and going to get credit with it or taking false loans. Nothing is coming up for a vote that we are currently aware of. If there is something the IP Committee wants, it needs to be ready to go before the Executive Council at the retreat.

C. Diversity Committee, Woody Pollack, Tampa
Nothing to report.

E. Intellectual Property Certification, Jeanne Seewald, Naples

We currently have 132 Board Certified Intellectual Property lawyers, out of a total 4,600 Florida Board certified lawyers. The IP Certification exam in May had 7 examinees. The tests were graded yesterday and results will be available in the fall. Yesterday was Jeanne Seewald's last meeting as Chair of this committee. Rick Fee will be the Chair and Ury Fischer will be Vice Chair. The next exam is scheduled for May 14, 2015. The application period is September 1, 2014 through October 31, 2014. IT is important to inform people that are applying either for certification or recertification that the application is intensive and that they should allot more time than they might otherwise expect to make sure the materials are timely submitted.

There will be a new process for the testing going forward. The new process includes a pre-test. Board Certified lawyers may get a call to take a pre-test.

The recertification for the 2009 class of Board Certified IP lawyers is coming up. The deadline for applying for recertification is August 15, 2014. Qualifications for recertification (including 45 hours of CLE) must be completed by July 31, 2014.

III. NEW BUSINESS

A. Committee ListServ

A listserv is up and Sam Lewis is hosting it. There is an option to receive a digest of the posts as opposed to all posts immediately upon submission.

B. AIPLA IP Law Associations Regional Roundtable – Woody Pollack, Tampa

AIPLA has begun regional roundtables in an effort to coordinate discussion and resources among regional intellectual property groups. The roundtable discussion took place on June 5, 2014. The AIPLA shared information about three bar councils: Europe, Japan, and China. Regional IP Sections may appoint 2 delegates to each of these at no cost, with a stated goal to assist in coordinating patent prosecution issues with international issues. The AIPLA also made us aware of an amicus brief notification network to receive notifications of appellate briefs on IP issues.

IV. SIXTH ANNUAL INTELLECTUAL PROPERTY SYMPOSIUM

We are searching for someone to chair the symposium as well as volunteers to help in its planning. Kimra Morris-Major will be the CLE Vice Chair of the IP Committee next year and will coordinate the symposium. We discussed venue and agreed that the symposium should continue its rotation around the state and be held in South Florida next year, with Ft. Lauderdale being a strong candidate to host. Concerning topics, given the recent Supreme Court activity on intellectual property matters, it

may be worthwhile for the Symposium group to focus the symposium on these developments.

V. OTHER BUSINESS

A. Vancouver Executive Council Retreat – Ury Fischer, Coral Gables
Canada has passed a new anti-spam law set to go into effect on July 1, 2014. The Gowlings firm has a 1 hour webinar available on their website. If enough IP members participate in the CLE, we may be able to apply for CLE credit through the Florida Bar.

B. Business Law Retreat – Mark Stein, Aventura
Registration is open for the Business Law Retreat in Naples and they are still looking for sponsors.

C. CLE
Tom McThenia and Robert Norway of GrayRobinson, PA in Orlando presented a 1 hour CLE updating us on recent IP decisions from the Supreme Court and the TTAB. The CLE course number is 1404811N.

D. Antitrust Board Certification – Jim Gale
Antitrust Board Certification is being broadened to "Antitrust and Trade Regulation" Board Certification which may include members of this committee. Substantial involvement (30%) for that certification will relate to covenants to restrain trade, exclusive dealing contracts, unfair methods of competition under FCC or other federal statutes (like the Lanham Act), FDUPTA, laws regulating unfair competition, false advertising, and privacy.

VI. ADJOURNMENT
Next meeting will be at the Retreat, Naples, Florida August 29, 2014 – September 1, 2014.

Computer Abuse and Data Recovery Act ("CADRA")(Aug. 3, 2014)

Electronic Commerce
Part V: Computer Abuse and Data Recovery Act

668.801 Short Title.

This part may be cited as the "Computer Abuse and Data Recovery Act."

668.802 Purposes.

The provisions of this part shall be construed liberally to promote the following policies:

(a) to protect owners, operators and lessees of computers used in the operation of a business from harm or losses caused by unauthorized access to protected computers; and/or

(b) to protect owners of information stored in protected computers used in the operation of a business from harm or losses caused by unauthorized access to protected computers.

668.803 Prohibited Acts.

Whoever knowingly and with intent to cause harm or loss –

(a) obtains information from a protected computer without authorization and as a result thereof causes harm or loss;

(b) causes the transmission of a program, code, or command without authorization to a protected computer, and as a result of such transmission, causes harm or loss; or

(c) traffics in any password, security code or token, key fob, access device or similar information or device through which access to a protected computer may be obtained without authorization;

shall be liable to the extent provided in s. 668.804 in a civil action to: (i) the owner of the information who uses the information in connection with the operation of a business in connection with the protected computer, or (ii) the owner, operator or lessee of the protected computer.

668.804 Remedies.

(a) A person bringing an action under s. 668.803 for a violation may:

(1) recover such person's actual damages, including lost profits and losses;
(2) recover the violator's profits that are not taken into account in computing actual damages and losses under s. 668.804(a)(1); and
(3) seek injunctive or other equitable relief from the court to: (i) prevent a violation of

s. 668.803, or (ii) recover the original and all copies of the information which is subject to the violation.

(b) In any action arising under this part, a court may award reasonable attorney's fees to the prevailing party according to the circumstances of the case.

(c) The remedies available for a violation of s. 668.803 are in addition to remedies otherwise available for the same conduct under federal or state law.

(d) A final judgment or decree rendered in favor of the state in any criminal proceeding concerning the conduct of the defendant which forms the basis for any criminal proceeding under chapter 815, shall estop the defendant in any action brought pursuant to s. 668.803 as to all matters as to which such judgment or decree would be an estoppel as if the plaintiff had been a party in the criminal action.

(e) A civil action filed under s. 668.803 shall be commenced within three years of the time the violation occurred or within three years of the time the violation was discovered or should have been discovered with the exercise of due diligence.

668.805 Definitions.

As used in this part, the term:

(a) "Computer" means an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility, data storage device or communications facility directly related to or operating in conjunction with such device.

(b) "Protected computer" means a computer, used in connection with the operation of a business and storing information, programs or code used in connection with the operation of a business, in which the information, programs or code can only be accessed through a technological access barrier such as a password, security code or token, key fob, access device, or similar measure.

(c) “Without authorization” means to circumvent a technological access barrier to a protected computer, without the express or implied permission of the owner, operator or lessee of the computer to access the protected computer or the express or implied permission of the owner of information stored in the protected computer, but does not include circumventing a technological measure that does not effectively control access to the protected computer or the information stored in the protected computer.

(d) "Harm" means any impairment to the integrity, access or availability of data, a program, a system, or information.

(e) "Loss" means any reasonable cost to the owner of information stored in a protected

computer or the owner, operator or lessee of a protected computer, including the reasonable cost of responding to the violation, conducting a damage assessment for harm associated with the violation, and remediation efforts including restoring the data, program, system, or information to its condition prior to the violation, and includes economic damages, lost profits, and consequential damages incurred because of interruption of service, and includes profits derived from a violation.

(f) "Traffics" means to sell, purchase or deliver.

(g) "Business" includes any trade or business without regard to its profit or nonprofit status.

668.806 Exclusions.

This part does not prohibit any lawfully authorized investigative, protective, or intelligence activity of any law enforcement agency, regulatory agency or political subdivision of this State, any other state, the United States or any foreign country.

Computer Abuse and Data Recovery Act (CADRA) White Paper - August 3, 2014

SUMMARY

The proposed Computer Abuse and Data Recovery Act (CADRA) protects owners, operators and lessees of protected computers and owners of information stored in protected computers from hackers and others who misappropriate passwords or override technologic access barriers in protected computers. CADRA is limited to business operations using protected computers which store business information. "Protected computers" are computers which are password protected or which utilize technological access barriers such as security codes, security tokens, key fobs or other access control devices for hardware, software or digital information.

WHY

Florida businesses need an effective civil remedies statute that provides redress for persons who, without authority, access or take computer data, or destroy computer data or systems. These violators might be insiders, such as disloyal employees or bad contractors, or they could be outsiders who hack into computers taking data and potentially destroying hardware, software and valuable data.

Currently, Florida's Computer Crimes Act, Fla. Stat. §. 815.01 et seq., ("Fla-CCA") is not a viable civil liability statute because, in order to support a claim for civil damages, the violator must be first convicted of a computer crime under the statute. Even if this is achieved, the Fla-CCA specifically excludes employees "acting in the scope of their lawful employment" and Florida courts have interpreted "acting in the scope of their lawful employment" to mean that if they EVER had authorized access, the statute does not apply even if they were no longer employees at the time of the access or if they used the data to intentionally harm the employer.

As for federal remedies, the Computer Fraud and Abuse Act, 18 U.S.C. § 1030, ("Fed-CFAA") covers similar issues and also provides for a civil remedy, if the damages exceed $5,000. Unlike the Fla-CCA, the Fed-CFAA has both an "unauthorized access" and "exceeds authorized access" cause of action. Like the Fla-CCA, the Fed-CFAA is primarily criminal in nature, and has been strictly construed by some regional federal appellate courts (the 9th and the 4th Circuits). These courts hold that if the accused has any type of authorized access to the data or computer, then he or she does not violate the Act. Other federal appellate courts (the 1st, 5th, and 7th Circuits), have given a broader interpretation of what is meant by "exceeds authorized access." The 11th Circuit seems to lean towards a broader interpretation of the Fed-CFAA, but the scope of the leading 11th Circuit decision is less than clear on this issue. The criminal conviction prerequisite in the Fla-CCA combined with the circuit split with some appellate courts finding no liability makes civil actions under Fed-CFAA increasingly difficult.

CADRA VIOLATIONS

A CADRA violation occurs when a person knowingly and with intent to cause harm or loss (a) obtains information from a protected computer without authorization and causes harm or loss; (b) causes transmission of a program, code or command without authorization to a protected computer and causes harm or loss or (c) traffics in any password, security code or access device through which access to a protected computer may be obtained without authorization. A person who violates Section 668.803(a), (b) or (c) is liable to the owner of the information used in his or her business stored in the protected computer or the owner, operator or lessee of the protected computer.

The injured party may bring a CADRA action seeking to recover actual damages including loss profits and losses and the violator's profits. The injured party may also seek injunctive or other equitable relief to prevent violation of CADRA and to recover the original and all copies of the information which is subject to the violation. This injunctive relief, for the original and all copies, is important in business disputes. Attorneys fees are available to the prevailing party according to the circumstances of the case. The action must be brought within three years of the violation or the reasonable discovery thereof.

CADRA defines the term "protected computer" as a computer storing information used in business when the information and/or the computer has a technological access barrier such as a password, security code or token, key fob, access device or other similar measure. The term "without authorization" means to circumvent the technological access barrier to the protected computer without the express or implied permission of the owner. "Without authorization" does not include circumventing a technological measure that does not effectively control access to the protected computer or the information stored therein. "Harm" is defined as including impairment to the integrity, access or availability of the data, program or information. A "loss" is any reasonable cost to the owner of the information or the owner of the protected computer, including the reasonable cost of responding to the violation, conducting a damage assessment and follow-on remediation efforts.

In conclusion, CADRA will provide Florida businesses with a civil remedy for computer-related abuses, including retrieval of programs, code and information and reasonable compensation for investigation and remediation of computer data-related losses.

Robert Kain, Esq.
Kain & Assoc.
Fort Lauderdale, Fl
rkain@ complexip.com
ofc. 954-768-9002

Computer Abuse and Data Recovery Act (CADRA) Legislative White Paper - August 21, 2014

Section 668.801: The title of the act is: the Computer Abuse and Data Recovery Act.

Section 668.802: The purpose and policy of the Act is to (a) protect owners, operators and lessees of computers used in a business from harm or loss caused by unauthorized access to protected computers and (b) protect owners of business information stored in protected computers from harm or loss caused by unauthorized access to protected computers.

Section 668.803: The Act is violated when a person knowingly and with intent to cause harm or loss (a) obtains information from a protected computer without authorization and causes harm or loss; or (b) causes the transmission of a program, code, or command without authorization to a protected computer and causes harm or loss; or (c) traffics in any password, security code or token, key fob, access device or similar information or device through which access to a protected computer may be obtained without authorization. Persons and organizations who may bring civil action against a violator include: (i) the owner of business information stored in a protected computer, or (ii) the owner, operator or lessee of a protected computer.

Section 668.804 sets forth the Act's civil remedies in sub-section (a) which include: (1) recovery of actual damages, lost profits and losses (defined in s. 668.804); (2) recovery of the violator's profits; and (3) injunctive or equitable to prevent a violation of the Act which includes recovery of the original and all copies of the subject information. Per sub-section (b), the court may award reasonable attorney's fees to the prevailing party. The Act's remedies are in addition to other remedies otherwise available (sub-section (c)). If the violator is criminally charged and convicted, he or she is estopped under the Act as to all matters as to which would be an estoppel as if the injured party plaintiff had been a party in the criminal action (sub-section (d)). Any action under the Act must be filed within three years of the violation or within three years after the violation was discovered or should have been discovered with diligence (sub-section (e)).

Section 668.8005 defines terms used in the Act. A "computer" is an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility, data storage device or communications facility directly related to or operating in conjunction with such device. A "protected computer" is a computer, used in connection with a business and storing information, programs or code used in the business, in which the information, programs or code can only be accessed through a technological access barrier such as a password, security code or token, key fob, access device, or similar measure. "Without authorization" means to circumvent a technological access barrier to a protected computer, without the express or implied permission of the owner, operator or lessee of the computer or the express or implied permission of the owner of information stored in the protected computer, but does not include circumventing a technological measure that does not effectively control access to the protected computer or the information stored in the protected computer. "Harm" means any impairment to the integrity, access or availability of data, a program, a system, or information. "Loss" means any reasonable

cost to the owner or the owner, operator or lessee of a protected computer, including the reasonable cost of responding to the violation, conducting a damage assessment, and remediation efforts including restoring the data, program, system, or information to its condition prior to the violation, and also includes economic damages, lost profits, and consequential damages incurred because of interruption of service, and profits derived from a violation. "Traffics" means to sell, purchase or deliver. "Business" is defined as including any trade or business without regard to its profit or nonprofit status.

Section 668.806 provides that certain actions of law enforcement agencies are exempt from the Act such as lawfully authorized investigative, protective, or intelligence activity of any law enforcement agency, regulatory agency or political subdivision of this State, any other state, the United States or any foreign country.

A bill to be entitled

An act relating to a fiduciary's access to digital assets; creating a new Chapter 740, entitled "Florida Fiduciary Access to Digital Assets Act"; defining terms used in the act; providing for the authority of the personal representative over digital assets of a decedent; providing for the authority of a guardian over the digital assets of a ward; providing for authority of an agent over digital assets of a principal pursuant to a power of attorney; providing for authority of a trustee over digital assets of a trust; providing for fiduciary's rights of access to digital assets; providing for custodian's duties as it relates to access; providing for immunity of the custodian for complying with this act; providing for applicability to existing relationships; and providing an effective date.

Be it Enacted by the Legislature of the State of Florida:

Section 1. Section 740.101, Florida Statutes, is created to read:

740.101. Short Title-- This chapter may be cited as the "Florida Fiduciary Access to Digital Assets Act."

Section 2. Section 740.201, Florida Statutes, is created to read:

740.201. Definitions-- As used in this chapter, the term:

(1) "Account holder" means:

(a) a person that has entered into a terms-of-service agreement with a custodian; and

(b) a fiduciary for a person described in subparagraph 1(a).

The term includes a deceased individual who entered into the agreement during the individual's lifetime.

(2) "Agent" means a person granted authority to act for a principal under a durable or nondurable power of attorney, whether denominated an agent, attorney in fact, or otherwise. The term includes an original agent, co-agent, and successor agent.

(3) "Carries" means engaging in the transmission of electronic communications.

(4) "Catalogue of electronic communications" means information that identifies each person with which an account holder has had an electronic communication, the time and date of the communication, and the electronic address of the person.

(5) "Content of an electronic communication" means information not readily accessible to the public concerning the substance or meaning of an electronic communication.

(6) "Court" means the circuit court.

(7) "Custodian" means a person that carries, maintains, processes, receives, or stores a digital asset of an account holder.

(8) "Digital asset" means a record that is electronic. The term does not include an underlying asset or liability to which an electronic record refers, unless the asset or liability is itself a record that is electronic.

(9) "Electronic" means technology having electrical, digital, magnetic, wireless, optical, electromagnetic, or similar capabilities.

(10) "Electronic communication" means a digital asset stored by an electronic-communication service or carried or maintained by a remote-computing service. The term includes the catalogue of electronic communications and the content of an electronic communication.

(11) "Electronic-communication service" means a custodian that provides to the public the ability to send or receive an electronic communication.

(12) "Fiduciary" means each person who is an original, additional, or successor personal representative, guardian, agent, or trustee.

(13) "Governing instrument" means a will, trust, instrument creating a power of attorney, or other dispositive, appointive, or nominative instrument.

(14) "Guardian" means a person who has been appointed by the court as guardian of the property of a minor or incapacitated person. The term includes a person who has been appointed by the court as an emergency temporary guardian of the property.

(15) "Information" means data, text, images, videos, sounds, codes, computer programs, software, databases, or the like.

(16) "Person" means an individual, estate, trust, business or nonprofit entity, public corporation, government or governmental subdivision, agency, or instrumentality, or other legal entity.

(17) "Personal representative" means the fiduciary appointed by the court to administer the estate of a deceased individual pursuant to letters of administration or an order appointing a curator or administrator ad litem for the estate.

(18) "Power of attorney" means a record that grants an agent authority to act in the place of a principal pursuant to Chapter 709.

(19) "Principal" means an individual who grants authority to an agent in a power of attorney.

(20) "Record" means information that is inscribed on a tangible medium or that is stored in an electronic or other medium and is retrievable in perceivable form.

(21) "Remote-computing service" means a custodian that provides to the public computer processing services or the storage of digital assets by means of an electronic communication system, as defined 18 U.S.C. 2510(14).

(22) "Terms-of-service agreement" means an agreement that controls the relationship between an account holder and a custodian.

(23) "Trustee" means a fiduciary that holds legal title to an asset pursuant to an agreement, declaration, or trust instrument that creates a beneficial interest in the settlor or others.

(24) "Ward" means a person for whom a guardian has been appointed.

(25) "Will" means an instrument admitted to probate, including a codicil, executed by a person in the manner prescribed by the Florida Probate Code, which disposes of the person's property on or after his or her death and includes an instrument which merely appoints a personal representative or revokes or revises another will.

Section 3. Section 740.301, Florida Statutes, is created to read:

740.301. Authority of Personal Representative over Digital Assets of a Decedent--Subject to Section 740.701(2) and unless otherwise provided by the court or the will of a decedent, a personal representative of the decedent has the right to access:

(1) the content of an electronic communication sent or received by the decedent if the electronic-communication service or remote computing service is permitted to disclose the content under the Electronic Communications Privacy Act, 18 U.S.C. Section 2702(b) [as amended];

(2) the catalogue of electronic communications sent or received by the decedent; and

(3) any other digital asset in which the decedent at death had a right or interest.

Section 4. Section 740.401, Florida Statutes, is created to read:

740.401. Authority of Guardian over Digital Assets of a Ward--The court, after an opportunity for hearing, may grant a guardian the right to access:

(1) the content of an electronic communication sent or received by the ward if the electronic-communication service or remote computing service is permitted to disclose the content under the Electronic Communications Privacy Act, 18 U.S.C. Section 2702(b) [as amended];

(2) the catalogue of electronic communications sent or received by the ward; and

(3) any other digital asset in which the ward has a right or interest.

Section 5. Section 740.501, Florida Statutes, is created to read:

740.501. Control By Agent of Digital Assets—

(1) To the extent a power of attorney expressly grants authority to an agent over the content of an electronic communication of the principal, the agent has the right to access the content of an electronic communication sent or received by the principal if the electronic-communication service or remote computing service is permitted to disclose the content under the Electronic Communications Privacy Act, 18 U.S.C. Section 2702(b) [as amended], and

(2) Except as provided in subsection (1) and unless otherwise provided by a power of attorney or a court, an agent has the right to access:

(a) the catalogue of electronic communications sent or received by the principal; and

(b) any other digital asset in which the principal has a right or interest.

Section 6. Section 740.601, Florida Statutes, is created to read:

740.601. Control By Trustee of Digital Assets-- Subject to Section 740.701(2) and unless otherwise provided by the court or the terms of a trust, a trustee or a successor of the trustee:

(1) that is an original account holder has the right to access each digital asset held in trust, including the catalogue of electronic communications sent or received and the content of an electronic communication; and

(2) that is not an original account holder has the right to access each digital asset held in trust as follows:

(a) the catalogue of electronic communications sent or received by the account holder; and

(b) the content of an electronic communication sent or received by the account holder if the electronic-communication service or remote computing service is permitted to disclose the content under the Electronic Communications Privacy Act, 18 U.S.C. Section 2702(b) [as amended];

(c) any other digital asset in which the account holder or any successor account holder has a right or interest.

Section 7. Section 740.701, Florida Statutes, is created to read:

740.701. Fiduciary Access and Authority--

(1) A fiduciary that is an account holder or has the right under this chapter to access a digital asset of an account holder:

(a) subject to the terms-of-service agreement and copyright or other applicable law, may take any action concerning the asset to the extent of the account holder's authority and the fiduciary's powers under the laws of this state;

(b) has, under applicable electronic privacy laws, the lawful consent of the account holder for the custodian to divulge the content of an electronic communication to the fiduciary; and

(c) is, under applicable computer fraud and unauthorized access laws, an authorized user.

(2) If a provision in a terms-of-service agreement limits a fiduciary's access to the digital assets of the account holder, the provision is void as against the strong public policy of this state, unless the account holder, after the effective date of this chapter, agreed to the provision by an affirmative act separate from the account holder's assent to other provisions of the terms-of-service agreement.

(3) A choice-of-law provision in a terms-of-service agreement is unenforceable against a fiduciary acting under this chapter to the extent the provision designates law that enforces a limitation on a fiduciary's access to digital assets which is void under subsection (2).

(4) Except as provided in subsection (2), a fiduciary's access under this chapter to a digital asset does not violate a terms-of-service agreement, notwithstanding a provision of the agreement, which limits third-party access or requires notice of change in the account holder's status.

(5) As to tangible personal property capable of receiving, storing, processing, or sending a digital asset, a fiduciary with authority over the property of a decedent, ward, principal, or settlor has the right to access the property and any digital asset stored in it and is an authorized user for purposes of any applicable computer fraud and unauthorized access laws, including the laws of this State.

Section 8. Section 740.801, Florida Statutes, is created to read:

740.801. Compliance--

(1) If a fiduciary with a right under this chapter to access a digital asset of an account holder complies with subsection (2), the custodian shall comply with the fiduciary's request in a record for:

(a) access to the asset;

(b) control of the asset; and

(c) a copy of the asset to the extent permitted by copyright law.

(2) If a request under subsection (1) is made by:

(a) a personal representative with the right of access under s. 740.301, the request must be accompanied by a certified copy of the letters of administration of the personal representative, an order authorizing a curator or administrator ad litem, , or other court order;

(b) a guardian with the right of access under s. 740.401, the request must be accompanied by a certified copy of letters of plenary guardianship of the property or a court order that gives the guardian authority over the digital asset;

(c) an agent with the right of access under s. 740.501, the request must be accompanied by a an original or a copy of the power of attorney that authorizes the agent to exercise authority over the digital asset and a certification of the agent, under penalty of perjury, that the power of attorney is in effect; and

(d) a trustee with the right of access under s. 740.601, the request must be accompanied by a certified copy of the trust instrument, or a certification of the trust under s. 736.1017, that authorizes the trustee to exercise authority over the digital asset.

(e) a person who is entitled to receive and collect specified digital assets pursuant to a certified copy of an order of summary administration issued pursuant to chapter 735, Florida Statutes.

(3) A custodian shall comply with a request made under subsection (1) not later than 60 days after receipt. If the custodian fails to comply, the fiduciary may apply to the court for an order directing compliance.

(4) A custodian that receives a certification of trust may require the trustee to provide copies of excerpts from the original trust instrument and later amendments which designate the trustee and confer on the trustee the power to act in the pending transaction.

(5) A custodian that acts in reliance on a certification of trust without knowledge that the representations contained in it are incorrect is not liable to any person for so acting and may assume without inquiry the existence of facts stated in the certification.

(6) A person that in good faith enters into a transaction in reliance on a certification of trust may enforce the transaction against the trust property as if the representations contained in the certification were correct.

(7) A person that demands the trust instrument in addition to a certification of trust or excerpts under subsection (4) is liable for damages if the court determines that the person did not act in good faith in demanding the trust instrument.

(8) This section does not limit the right of a person to obtain a copy of a trust instrument in a judicial proceeding concerning the trust.

Section 9. Section 740.901, Florida Statutes, is created to read:

Section 740.901. Custodian Immunity--A custodian and its officers, employees, and agents are immune from liability for any action done in good faith in compliance with this chapter.

Section 10. Section 740.1001, Florida Statutes, is created to read:

Section 740.1001. Relation to Electronic Signatures in Global and National Commerce Act--This chapter modifies, limits, or supersedes the Electronic Signatures in Global and National Commerce Act, 15 U.S.C. Section 7001 et seq., but does not modify, limit, or supersede Section 101(c) of that act, 15 U.S.C. Section 7001(c), or authorize electronic delivery of any of the notices described in Section 103(b) of that act, 15 U.S.C. Section 7003(b).

Section 11. Section 740.1101, Florida Statutes, is created to read:

Section 740.1101. Applicability-- This chapter applies to:

(1) Subject to subsection (2), this chapter applies to:

(a) an agent acting under a power of attorney executed before, on, or after the effective date of this chapter;

(b) a personal representative acting for a decedent who died before, on, or after the effective date of this chapter;

(c) a guardian appointed through a guardianship proceeding, whether pending in a court or commenced before, on or after the effective date of this chapter; and

(d) a trustee acting under a trust created before, on, or after the effective date of this chapter.

(2) This chapter does not apply to a digital asset of an employer used by an employee in the ordinary course of the employer's business.

Section 12. This act shall take effect July 1, 2015.

WHITE PAPER

PROPOSED ENACTMENT OF CHAPTER 740, FLORIDA STATUTES

I. SUMMARY

The proposed legislation is a result of a study by the Digital Assets Committee of The Real Property, Probate and Trust Law Section of The Florida Bar of recent work on a Uniform Fiduciary Access to Digital Assets Act. The proposal would add a new Chapter to the Florida Statutes that follows the proposed uniform act.

Under present Florida law, there is no legislation on fiduciary access to digital assets, only criminal laws regarding access to stored communications. The purpose of this act is to vest fiduciaries with the authority to access, control, or copy digital assets and accounts. The Florida Fiduciary Access to Digital Assets Act ("FFADAA") addresses four different types of fiduciaries: personal representatives of decedents' estates, guardians of the property of minors or incapacitated persons, agents acting pursuant to a power of attorney, and trustees.

II. CURRENT SITUATION

As the number of digital assets held by the average person increases, questions surrounding the disposition of these assets upon the individual's death or incapacity are becoming more common. These assets range from online gaming items to photos, to digital music, to client lists. And these assets have real value: according to a 2011 survey from McAfee, Intel's security-technology unit, American consumers valued their digital assets, on average, at almost $55,000.[1] Few holders of digital assets and accounts consider the fate of their online presences once they are no longer able to manage their assets. There are millions of Internet accounts that belong to decedents. Some Internet service providers have explicit policies on what will happen when an individual dies, others do not; even where these policies are included in the terms of service, most consumers click through these agreements. Few laws exist on the rights of fiduciaries over digital assets.

The **current federal legislation** that dictates access to digital assets is buried in the Stored Communications Act ("SCA") and the Computer Fraud and Abuse Act ("CFAA"), both passed in 1986, with only minor revisions since. The CFAA and similar state laws impose criminal penalties and perhaps civil liability too for the unauthorized access of computer hardware, devices, and stored data. These laws are explained in more detail below.

---

[1] Kelly Greene, *Passing Down Digital Assets*, WALL STREET JOURNAL (Aug. 31, 2012), http://goo.gl/7KAaOm.

Under **current Florida law**, Florida has enacted statutory counterparts to the provisions of the SCA and located them in Chapter 934, entitled "Security of Communications"[2] and in Chapter 815, entitled “Florida Computer Crimes Act”. There is no legislation on fiduciary access to digital assets.

A minority of **other states** has enacted legislation on fiduciary access to digital assets, including Connecticut, Idaho, Indiana, Oklahoma, Rhode Island, Nevada, and Virginia, and the existing statutes grant varying degrees of access to different types of digital assets. In addition, numerous other states have considered, or are considering, legislation. Existing legislation differs with respect to the types of digital assets covered, the rights of the fiduciary, the category of fiduciary included, and whether the principal’s death or incapacity is covered.

The **National Conference of Commissioners on Uniform State Laws** at its annual conference this July passed the **Uniform Fiduciary Access to Digital Assets Act** (the “UFADAA”). The Act specifically addresses how a fiduciary addresses digital assets. The commissioners on the drafting committee received input from estate attorneys, educators, and lawyers with expertise in various areas of the law affected by digital assets, advisors from the American Bar Association, representatives from service providers, such as Facebook and Yahoo, policy counsel from NetChoice (a trade association of eCommerce businesses and on-line consumers), and General Counsel from the State Privacy and Security Coalition, Inc. (which is comprised of 20 communications, technology, and media companies).[3]

The UFADAA took into account the **Supremacy Clause of the U.S. Constitution**. According to the Supremacy Clause, "This Constitution, and the laws of the United States which shall be made in pursuance thereof.... *shall be the supreme law of the land,* and the judges in every state shall be bound thereby, anything in the Constitution or laws of any State to the contrary, notwithstanding."[4] The Supreme Court has ruled that a federal law that conflicts with a state law "preempts" the state law and that state laws that conflict with federal law are "without effect."[5] Due to the Supremacy Clause and the Supreme Court’s interpretation, one major challenge in drafting the uniform act was that it does not directly conflict with existing federal law and could survive a constitutional challenge.[6]

It is what the **SCA** *does not specifically address* that gave rise to the UFADAA proposed state law that the Uniform State Laws Commissioners believed can be legally interpreted as filling in the gaps of the SCA, as opposed to conflicting with it. The SCA was originally written to provide Fourth Amendment-like[7] privacy protection for certain types

---

[2] *Tracey v. State, 69 So.3d 992* (Fla. 4th DCA 2011).

[3] “Surf the Evolving Web of Laws Affecting Digital Assets” Bissett, W. and Kauffman, D. 41 Estate Planning No. 4 April 2014.

[4] U.S. Const. Art. VI (Emphasis added.)

[5] Maryland v. Louisiana, 451 U.S, 725 (1981).

[6] “Surf the Evolving Web” at 34.

[7] The Fourth Amendment to the U.S. Constitution protects the "people’s rights to be secure in their houses, *papers, and effects,* against unreasonable searches and seizures." (Emphasis added.)

of email communications, social networking accounts, and other digital assets stored on a remote server. "The SCA attempts to modernize the reasonable expectation of privacy provided by the Fourth Amendment and later the Supreme Court to include two types of online services, "electronic communication services" and "remote computing services". To provide this privacy protection, the SCA limits the ability of the government to *compel disclosure* of both "non-content" information (i.e., logs of email communications including addresses of recipient/senders (analogous to the envelope of a letter)) as well as the "content" (what is inside the letter). The SCA also limits the ability of those internet service providers ("ISPs") that are "subject to" the SCA to reveal "content" information to non-government entities."[8] In general, the SCA states that certain service providers are permitted to disclose "non-content" information of electronic communications and files to anyone except the government without the consent of the user. However, a service provider *may* divulge the "content" of an electronic communication to a non-government entity *only* when the account holder lawfully consents.[9]

Like the SCA, the **CFAA** similarly protects against anyone who "intentionally accesses a computer without authorization or exceeds authorized access." Neither the SCA nor the CFAA specifically provides for or denies a fiduciary access to electronic and stored communications. In essence, even if consent was granted to a fiduciary, current federal law does not acknowledge the potential for such a vested right.[10]

The UFADAA uses well-established, existing law for non-digital probate assets in order to provide **a fiduciary the right to "step into the shoes"** of a decedent to manage digital assets. Because the interest to properly administer both non-digital and digital estate assets are similar, a fiduciary should be granted the same authority over both types of property. Because the fiduciary has the same authority as the deceased account holder (no more and no less), the fiduciary is "authorized" by the deceased account holder as required under the two federal statutes (the SCA and CFAA) that prohibit unauthorized access.

The UFADAA was also drafted in light of the fact that deceased account holders likely registered with on-line services for email, on-line purchases, photo sharing, on-line banking, and a long list of other items now done on-line by first consenting to a terms-of service agreement ("TOSA"). The UFADAA recognized that in most situations the account holder likely consented to the TOSA by clicking "I agree" without ever reading it. These TOSAs generally describe the account holder's rights in using the service, how personal information will be protected, the conditions on information sharing, and account holder's rights (if any) upon death. The UFADAA has taken into account a service provider's possible refusal to grant fiduciary access simply because the deceased account holder consented to (a likely unread) blanket TOSA by writing the uniform act such that fiduciary access, by itself, will not be deemed a violation of a TOSA or deemed an unauthorized transfer of an account.[11]

---

[8] "Surf the Evolving Web" at 34 (citations omitted).
[9] 18 U.S.C. section 2702(b)(3).
[10] "Surf the Evolving Web" at 34 (citations omitted).
[11] "Surf the Evolving Web" at 34 (citations omitted).

Because of issues like the federal Supremacy Clause and the interest of ISPs in differing jurisdictions, the Florida drafting committee closely adhered to the careful analysis and drafting set forth within the UFADAA, deviating from the proposed uniform law minimally, only where necessary to comport with Florida law.

III. EFFECT OF PROPOSED CHANGES

A. **Effect of the Proposed Changes.** It is important to understand that the goal of the FFADAA is to remove barriers to a fiduciary's access to electronic records and that the federal and state substantive rules of fiduciary, probate, trust, banking, security, and agency law remain unaffected by FFADAA. The act applies only to fiduciaries that act in compliance with their fiduciary powers. It distinguishes the authority of fiduciaries—which exercise authority subject to this act only on behalf of the account holder—from any other efforts to access the digital assets. Family members or friends may seek such access, but, unless they are fiduciaries, their efforts are subject to other laws and are not covered by this act.

This Act follows mirros the UFADAA because a uniform approach among states will provide certainty and predictability for courts, account holders, fiduciaries, and ISPs. The uniform act gives states precise, comprehensive, and easily accessible guidance on questions concerning fiduciaries' ability to access the electronic records of a decedent, protected person, principal, or a trust. Additionally, ISPs have participated in the drafting of the UFADAA and, presumably, find the proposed act to be acceptable.

The general goal of the FFADAA is to facilitate fiduciary access while respecting the privacy and intent of the account holder. It adheres to the traditional approach of trusts and estates law, which respects the intent of the account holder and promotes the fiduciary's ability to administer the account holder's property. With regard to the general scope of the act, the act's coverage is inherently limited by the definition of "digital assets." The act applies only to electronic records. The term does not include the underlying asset or liability unless it is itself an electronic record.

B. The act is divided into **twelve sections**.

1. **Section 740.101** contains the short title of the Act.

2. **Section 740.201** contains general provisions and definitions, including those relating to the scope of the fiduciary's authority.

The definitions of "agent", "guardian", "court", "electronic", "fiduciary", "governing instrument", "person", "personal representative", "power of attorney", "principal", "record", "trustee", "ward", and "will" are based on those found in applicable Florida law, such as the Florida Probate Code and Florida Powers of Attorney Act.

UFADAA Uniform Act	Florida Statutes
Section .201 Definitions	
(2) Agent	709.2102(1)
(6) Court	731.201(7)
(9) Electronic	709.2102(5)
(12) Fiduciary	739.102(6), 738.102 (4), 733.817, 518.10
(13) Governing Instrument	732.2025(4)
(14) Guardian	744.604(6)
(16) Person	1.01(3)
(17) Personal Representative	731.201(28)
(18) Power of Attorney	709.2102(7)
(19) Principal	709.2102(9)
(20) Record	709.2102(13)
(23) Trustee	731.201(39)
(24) Ward	744.102(22)
(25) Will	731.201(40)

The other definitions are new for this Act, although the definition of digital service comes from the White House Digital Government Strategy: http://www.whitehouse.gov/sites/default/files/omb/egov/digital-government/digital-government-strategy.pdf. The definition of "contents" is adapted from 18 U.S.C. § 2510(8); the definition of "electronic communication" is adapted from the language of 18 U.S.C. §§ 2510(12) and 2702(a)(1) and (2); the definition of "electronic communication service" is drawn from 18 U.S.C. 2510(15); and the definition of "remote computing service" is adapted from 18 U.S.C. § 2711(2), to help ensure the Act's compliance with federal law.

The Act includes a definition for "catalogue of electronic communications." This is designed to cover log-type information about an electronic communication. The term "content of an electronic communication" is adapted from 18 U.S.C. § 2510(8), but it refers only to information that is not readily accessible to the public because, if the information were readily accessible to the public, it would not be subject to the privacy protections of federal law under the Electronic Communications Privacy Act ("ECPA"), 18 U.S.C. §§ 2510 et seq. See S. Rep. No. 99-541, at 36 (1986). When the privacy protections of federal law under ECPA apply to the content of an electronic communication, the ECPA's legislative history notes the requirements for disclosure: "Either the sender or the receiver can directly or through authorized agents authorize further disclosures of the contents of their electronic communication." S. Rep. No. 99-541, at 37 (1986)).

ECPA does not apply to private e-mail service providers, such as employers and educational institutions.[12]

[12] See 18 U.S.C. §2702(a)(2); James D. Lamm, Christina L. Kunz, Damien A. Riehl, & Peter John Rademacher, *The Digital Death Conundrum: How Federal and State Laws Prevent Fiduciaries from Managing Digital Property*, 68 U. Miami L. Rev. 385, 404 (2014) (available at: http://goo.gl/T9jX1d).

A "custodian" includes any internet service provider as well as any other entity that provides or stores electronic data of an account holder. The term "carries" means engaging in the transmission or switching of electronic communications. See 47 U.S.C. § 1001(8). A custodian does not include most employers because an employer typically does not have a terms-of-service agreement with an employee. Any digital assets created through employment generally belong to the employer.

Example -- Fiduciary access to an employee email account. D dies, employed by Company Y. Company Y has an internal email communication system, available only to Y's employees. D's personal representative, R, believes that D used Company Y's email system for some financial transactions that R cannot find through other means. R requests access from Company Y to the emails.

Company Y is not a custodian subject to the act. Under Section .201(6), a custodian must carry, maintain or store an account holder's digital assets. An account holder, in turn, is defined under Section .201(1) as someone who has entered into a terms-of-service agreement. Company Y, like most employers, did not enter into a terms-of-service agreement with D, so D was not an account holder.

"Digital assets" include products currently in existence and yet to be invented that are available only electronically. Digital assets include electronically-stored information, such as: 1) any information stored on a computer and other digital devices; 2) content uploaded onto websites, ranging from photos to documents; and 3) rights in digital property, such as domain names or digital entitlements associated with online games.[13] Both the catalogue and content of an electronic communication are covered by the term "digital assets."

The fiduciary's access to a record defined as a "digital asset" does not mean that the fiduciary is entitled to "own" the asset or otherwise engage in transactions with the asset. Consider, for example, funds in a bank account or securities held with a broker or other custodian, regardless of whether the bank, broker, or custodian has a brick-and-mortar presence. This Act affects records concerning the bank account or securities, but does not affect the authority to engage in transfers of title or other commercial transactions in the funds or securities, even though such transfers or other transactions might occur electronically. The Act reinforces the right of the fiduciary to access all relevant electronic communications and the online account that provides evidence of ownership. Thus, an entity may not refuse to provide access to online records any more than the entity can refuse to provide the fiduciary with access to hard copy records.

The definition of "electronic communication" is adapted from the language of 18 U.S.C. §§ 2510(12) and 2702(a)(1) and (2); the definition of "electronic-communication service" is drawn from 18 U.S.C. § 2510(15); and the definition of "remote-computing service" is adapted from 18 U.S.C. § 2711(2), to help ensure the

[13] See Lamm, et al, supra, at 388.

Act's compliance with federal law. Electronic communication is a subset of digital assets and covers only the category of digital assets subject to the privacy protections of the ECPA. For example, material stored on a computer's hard drive is a digital asset but not an electronic communication.

A "fiduciary" under this chapter occupies a status recognized by Florida law, and fiduciaries' powers under the chapter are subject to the relevant limits established by other state laws.

The "terms-of-service agreement" ("TOSA") definition relies on the definition of "agreement" found in UCC § 1-201(3) and that found in UCC § 1-201(b) (3) ("the bargain of the parties in fact, as found in their language or inferred from other circumstances, including course of performance, course of dealing, or usage of trade"). It refers to any agreement that controls the relationship between an account holder and a custodian, even though it might be called a terms-of-use agreement, a click-wrap agreement, a click-through license, or a similar term. State and federal law determine capacity to enter into a binding terms-of-service agreement.

3. **Section 740.301** establishes the rights of personal representatives. A personal representative is presumed to have access to all of the decedent's digital assets unless that is contrary to the decedent's will or to other applicable law.

This section establishes the default rule that the personal representative is authorized to access all of the decedent's digital assets other than material covered by the ECPA. The subsection clarifies the difference between fiduciary authority over digital assets other than electronic communications protected by ECPA, and authority over ECPA-covered electronic communications. For electronic communications, subsections (1) and (2) establish procedures that cover: first, the ECPA-covered content of communications and, second, the catalogue (logs and records) that electronic communications service providers may release without consent under the ECPA. Federal law distinguishes between the permissible disclosure of the "contents" of a communication, covered in 18 U.S.C. § 2702(b), and of "a record or other information pertaining to a" subscriber or customer, covered in 18 U.S.C. § 2702(c).[14]

Content-based material can, in turn, be divided into two types of communications: those received by the account holder and those sent. Material when the account holder is the "addressee or intended recipient" can be disclosed either to that individual or to an agent for that person, 18 U.S.C. § 2702(b)(1), and it can also be disclosed to third parties with the "lawful consent" of the addressee or intended recipient. 18 U.S.C. § 2702(b)(3). Material for which the account holder is the "originator" can only be disclosed to third parties with the account holder's "lawful consent." 18 U.S.C. § 2702(b)(3). (Note that, when the account holder is the addressee or intended recipient, material can be disclosed under either § 2702(b)(1) or (b)(3), but that when the account holder is the originator, lawful consent is required.) By contrast to content-based material, non-content material

[14] See Matthew J. Tokson, *The Content/Envelope Distinction in Internet Law*, 50 Wm. & Mary L. Rev. 2105 (2009).

can be disclosed not only with the lawful consent of the account holder but also to any person other than a governmental entity (which would presumably include fiduciaries). This information includes material about any communication sent, such as the addressee, sender, date/time, and other subscriber data, what this Act defines as the "catalogue of electronic communication". (Further discussion of this issue and examples are set out in the comments to Section .701, *infra*.)

4. **Section 740.401** establishes the rights of guardians. A guardian may access the assets pursuant to letters of guardianship or a court order.

This section establishes that the guardian must be specifically authorized by the court to access the ward's digital assets and electronic communications. Each of the different levels of access must be specifically granted by court order. The requirement for express authority over digital assets does not limit the fiduciary's authority over the underlying "bricks and mortar" assets, such as a bank account. As a legislative enacting matter, the meaning of the term "hearing" will vary, depending on a state's procedures.

Section .401 is comparable to Section .301. It responds to the concerns of ISPs who believe that the Act should be structured to clarify the difference between fiduciary authority over digital assets other than electronic communications protected by federal law (the ECPA) and fiduciary authority over ECPA-protected electronic communications. Consequently, this Act sets out procedures that cover all digital assets as well as the catalogue of electronic communications (logs and records) that providers may release without consent under ECPA, and then addresses ECPA-covered communications.

Under Section .401, the guardian has the same power over digital assets as the account holder. The guardian must exercise authority in the best interests of the ward pursuant to Chapter 744.

5. **Section 740.501** establishes the rights of agents acting pursuant to a power of attorney. An agent acting pursuant to a power of attorney is presumed to have access to all of a principal's digital assets not subject to the protections of other applicable law; if another law protects the asset, then the power of attorney must explicitly grant access.

This section establishes that the agent has default authority over the principal's digital assets and the records, other than the contents, of the principal's electronic communications. When the principal does not want the agent to exercise this authority, then the power of attorney must explicitly prevent an agent from doing so.

With respect to the contents of electronic communications, the agent must be specifically authorized by the principal to access the contents of the principal's electronic communications. Because a power of attorney contains the consent of the account holder, ECPA should not prevent the agent from exercising authority over the content of electronic communications. There should be no question that an explicit delegation of authority in a power of attorney constitutes authorization from the account holder to access digital assets, and provides "lawful consent" to allow disclosure of electronic

communications from an electronic communication service or a remote computing service pursuant to applicable law. Both authorization and lawful consent are important because 18 U.S.C. § 2701 deals with intentional access without authorization and 18 U.S.C. § 2702 allows a provider to disclose with lawful consent.

The uniform law commissioners considered whether the authority over digital assets and electronic communications should be a default power. They decided that the power to access the contents of electronic communications must be expressly granted, because when expressed and not default, it satisfies the lawful consent requirement of ECPA. The agent has default authority over other digital assets under the Act.

6. **Section 740.601** establishes the rights of trustees. A trustee may access any digital asset held by the trust unless that is contrary to the terms of the trust or to other applicable law

Access to digital assets, including the contents of the electronic communications, is presumed with respect to assets for which the trustee is the initial account holder. A trustee may have title to digital assets and electronic communications when the trust itself becomes the account holder of a digital asset held by the trust, and when the trustee becomes an account holder for trustee business, situations addressed in subsection (1).

Subsection (2) addresses situations involving either an inter vivos transfer of a digital asset into a trust or transfer via a pour-over will of a digital asset into a trust. There should be no question that holding property in trust form constitutes authorization from the account holder for the trustee to access digital assets, including both the catalogue and contents of the electronic communications, and this provides "lawful consent" to allow disclosure of electronic communications from an electronic communication service or a remote computing service pursuant to applicable law. Nonetheless, subsection (2) distinguishes between the catalogue and contents of electronic communications in case there are any questions about whether the form in which property – transferred into a trust - is held constitutes lawful consent. Both authorization and lawful consent are important because 18 U.S.C. § 2701 deals with intentional access without authorization, and 18 U.S.C. § 2702 allows a provider to disclose with lawful consent.

The underlying trust documents and the Florida Trust Code will supply the allocation of responsibilities between and among trustees.

7. **Section 740.701** contains provisions relating to the rights of the fiduciary to access digital assets.

This section clarifies that the fiduciary has the same authority as the account holder if the account holder were the one exercising the authority (note that, where the account holder has died, this means that the fiduciary has access as of the hour before the account holder's death). This means that the fiduciary's authority to access the digital asset is the same as the account holder except where, pursuant to subsection (2), the account holder has explicitly opted out of fiduciary access. Of course, in exercising its

responsibilities, the fiduciary is subject to the duties and obligations established pursuant to Florida law and is liable for breach of those duties.

This issue concerning the parameters of the fiduciary's authority potentially arises in two situations: 1) the fiduciary obtains access to a password directly from the account holder, as would be true in various circumstances such as for the trustee of an inter vivos trust or someone who has stored passwords with a digital locker and those passwords are then transmitted to the fiduciary; and 2) the fiduciary has obtained access pursuant to this Act.

The fiduciary does not, however, obtain power over any digital assets if that property was illegally obtained by the account holder. Note that even if the digital asset were illegally obtained by the account holder, the fiduciary would still need access in order to handle that asset appropriately. There may, for example, be tax consequences that the fiduciary would be obligated to report.

The section also provides that control by a fiduciary should not be considered a transfer that would violate the anti-transfer terms of a terms-of-service agreement. Finally, the fiduciary has the same responsibilities as the account holder more generally. For example, a fiduciary cannot delete an account if this would be fraudulent. Similarly, if the account holder could challenge provisions in a terms-of-service agreement, then the fiduciary is similarly able to do so.[15]

Subsection (1) is designed to establish that the fiduciary is authorized to exercise control over digital assets in accordance with other applicable laws. The language mirrors that used in Title II of the ECPA, known as the Stored Communications Act (SCA), 18 U.S.C. § 2701 *et seq.* The subsection clarifies that the fiduciary is "authorized" under the two federal statutes that prohibit unauthorized access to computers and computer data, the SCA and the CFAA,[16] as well as pursuant to any comparable state laws criminalizing unauthorized access.[17]

The Stored Communications Act contains two potentially relevant prohibitions.

(a) 18 U.S.C. § 2701(a), which concerns access to the digital assets, makes it a crime for anyone to "intentionally access without authorization a facility through which

---

[15] See *Ajemian v. Yahoo!, Inc*., 987 N.E.2d 604 (Mass. 2013).

[16] Stored Communications Act, 18 U.S.C. § 2701 *et seq*. (2006); Computer Fraud and Abuse Act, 18 U.S.C. § 1030 *et seq*. (2006); *see, e.g.,* Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 GEO. WASH. L. REV. 1208 (2004); Allan D. Hankins, Note, *Compelling Disclosure of Facebook Content Under the Stored Communications Act*, 17 SUFFOLK J. TRIAL & APP. ADVOC. 295 (2012).

[17] *See Computerized Hacking and Unauthorized Access States Laws*, NATIONAL CONFERENCE OF STATE LEGISLATURES (May 21, 2009), http://www.ncsl.org/issues-research/telecom/computer-hacking-and-unauthorized-access-laws.aspx; Christina Kunz, Peter Rademacher & Lucie O'Neill, 50 State Survey of Unauthorized Access (2012) (on file with the Committee and available on the Google Drive); James D. Lamm, et al., *The Digital Death Conundrum: How Federal and State Laws Prevent Fiduciaries from Managing Digital Property*, 68 U. Miami L. Rev. __ (2013), http://lawreview.law.miami.edu/wp-content/uploads/2011/12/The-Digital-Death-Conundrum-How-Federal-and-State-Laws-Prevent-Fiduciaries-from-Managing-Digital-Property.pdf.

an electronic communication service is provided" as well as to "intentionally exceed an authorization to access that facility." Thus, someone who has authorization to access the facility is not engaging in criminal behavior. Moreover, this section does not apply to "conduct authorized . . . by a user of that service with respect to a communication of or intended for that user."[18]

(b) 18 U.S.C. § 2702, "Voluntary disclosure of customer communications or records," concerns actions by the service provider. It prohibits an electronic communication service or a remote computing service from knowingly divulging the contents of a communication that is stored by or carried or maintained on that service unless disclosure is made (among other exceptions) "to an addressee or intended recipient of such communication or an agent of such addressee or intended recipient" or "with the *lawful consent* of the originator or an addressee or intended recipient of such communication, or the subscriber in the case of remote computing service."[19] The statute permits disclosure of "customer records" that do not include content, either with lawful consent from the customer or "to any person other than a governmental entity."[20] Thus, unlike the contents, the provider is permitted to disclose the non-content "records" of the electronic communications to anyone except the government, and may disclose to the government with the customer's lawful consent or in certain emergencies.

The Computer Fraud and Abuse Act prohibits unauthorized access to computers. 18 U.S.C. § 1030. Like the SCA, the CFAA similarly protects against anyone who "intentionally accesses a computer without authorization or exceeds authorized access." 18 U.S.C. § 1030(a).

Florida laws prohibit unauthorized access. See Chapters 815 and 934, Florida Statutes.

By defining the fiduciary as an authorized user: 1) the fiduciary has authorization to access the files under the *first* section of the SCA, 18 U.S.C. § 2701, as well as under the CFAA; and 2) the fiduciary has "the lawful consent" of the originator/subscriber so that the provider can voluntarily disclose the files pursuant to the *second* relevant provision of the SCA, 18 U.S.C. § 2702. Moreover, this language should be adequate to avoid liability under the Florida unauthorized access laws.

Subsection (4) reinforces the concept that the fiduciary "steps into the shoes" of the account holder, with no more – and no fewer – rights. For example, the TOSA controls the rights of the account holder (settlor, principal, incapacitated person, decedent). The Act does not permit the account holder's fiduciary to override the TOSA in order to make a digital asset or collection of digital assets "descendible," although it does preserve the rights of the fiduciary to make the same claims as the account holder.[21]

---

[18] 18 U.S.C. §§ 2701(a), (c)(2).
[19] 18 U.S.C. § 2702(b)(1), (3) (emphasis added).
[20] 18 U.S.C. § 2702(c)(2) and (6).
[21] See *Ajemian v. Yahoo!, Inc*., 987 N.E.2d 604 (Mass. 2013); David Horton, *Indescendibility*, 102 Calif. L. Rev. __ (forthcoming 2014), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2311506.

Subsection (5) is designed to clarify that the fiduciary is authorized to access digital assets stored on equipment of the decedent, ward, principal, or settlor, thereby superseding Florida laws on unauthorized access to the equipment.

Example 1 – Access to digital assets by personal representative. D dies with a will that is silent with respect to digital assets. D has a bank account for which D received only electronic statements, D has stored photos in a cloud-based Internet account, and D has an e-mail account with a company that provides electronic-communication services to the public. The personal representative of D's estate needs access to the electronic bank account statements, the photo account, and e-mails.

The personal representative of D's estate has the authority to access D's electronic banking statements and D's photo account, which both fall under the act's definition of a "digital asset." This means that, if these accounts are password-protected or otherwise unavailable to the personal representative, then the bank and the photo account service must give access to the personal representative when the request is made in accordance with Section .801. If the TOSA permits D to transfer the accounts electronically, then the personal representative of D's estate can use that procedure for transfer as well.

The personal representative of D's estate is also able to request that the e-mail account service provider grant access to e-mails sent or received by D; ECPA permits the service provider to release the catalogue to the personal representative. The service provider also must provide the personal representative access to the content of an electronic communication sent or received by D if the service provider is permitted under 18 U.S.C. Section 2702(b) to disclose the content. The bank may release the catalogue of electronic communications or content of an electronic communication for which it is the originator or the addressee because the bank is not subject to the ECPA.

Example 2 – Access to digital assets by guardian. C is seeking appointment as the guardian for P. P has a bank account for which P received only electronic statements, P has stored photos in a cloud-based Internet account, and P has an e-mail account with a company that provides electronic communication services to the public. C needs access to the electronic bank account statements, the photo account, and e-mails.

Without a court order that explicitly grants access to P's digital assets, including electronic communications, C has no authority pursuant to this Act to access the electronic bank account statements, the photo account, or the e-mails. Based on law outside of this Act, the bank may release the catalogue of electronic communications or content of an electronic communication for which it is the originator or the addressee because the bank is not subject to the ECPA.

Example 3 – Access to digital assets by agent. X creates a power of attorney designating A as X's agent. The power of attorney expressly grants A authority over X's

digital assets, including the content of an electronic communication. X has a bank account for which X receives only electronic statements, X has stored photos in a cloud-based Internet account, and X has a game character and in-game property associated with an online game. X also has an e-mail account with a company that provides electronic-communication services to the public.

A has the authority to access X's electronic bank statements, the photo account, the game character and in-game property associated with the online game, all of which fall under the act's definition of a "digital asset." This means that, if these accounts are password-protected or otherwise unavailable to A as X's agent, then the bank, the photo account service provider, and the online game service provider must give access to A when the request is made in accordance with Section .801. If the TOSA permits X to transfer the accounts electronically, then A as X's agent can use that procedure for transfer as well.

As X's agent, A is also able to request that the e-mail account service provider grant access to e-mails sent or received by X; ECPA permits the service provider to release the catalogue. The service provider also must provide A access to the content of an electronic communication sent or received by X if the service provider is permitted under 18 U.S.C. Section 2702(b) to disclose the content. The bank may release the catalogue of electronic communications or content of an electronic communication for which it is the originator or the addressee because the bank is not subject to the ECPA.

Example 4 – Access to digital assets by trustee. T is the trustee of a trust established by S. As trustee of the trust, T opens a bank account for which T receives only electronic statements. S transfers into the trust to T as trustee (in compliance with a TOSA) a game character and in-game property associated with an online game and a cloud-based Internet account in which S has stored photos. S also transfers to T as trustee (in compliance with the TOSA) an e-mail account with a company that provides electronic-communication services to the public.

T is an original account holder with respect to the bank account that T opened, and T has the ability to access the electronic banking statements. T, as successor account holder to S, may access the game character and in-game property associated with the online game and the photo account, which both fall under the act's definition of a "digital asset." This means that, if these accounts are password-protected or otherwise unavailable to T as trustee, then the bank, the photo account service provider, and the online game service provider must give access to T when the request is made in accordance with Section .801. If the TOSA permits the account holder to transfer the accounts electronically, then T as trustee can use that procedure for transfer as well.

T as successor account holder of the e-mail account for which S was previously the account holder is also able to request that the e-mail account service provider grant access to e-mails sent or received by S; the ECPA permits the service provider to release the catalogue. The service provider also must provide T access to the content of an electronic communication sent or received by S if the service provider is permitted under 18 U.S.C. Section 2702(b) to disclose the content. The bank may release the catalogue of

electronic communications or content of an electronic communication for which it is the originator or the addressee because the bank is not subject to the ECPA.

Example 5 – Access notwithstanding terms in a TOSA. D, who is domiciled in Florida, dies. D was a professional photographer who stored valuable digital photos in an online storage account provided by C. P is appointed by a court in Florida to administer D's estate. P needs access to D's online storage account to inventory and appraise D's estate assets and to file D's estate tax return. During D's lifetime, D entered into a TOSA with C for the online storage account. The choice-of-law provision selects the law of state Y to govern the contractual rights and duties under the TOSA. A provision of the TOSA prohibits fiduciary access to the digital assets of an account holder, but D did not agree to that provision by an affirmative act separate from D's assent to other provisions of the TOSA. FFADAA has been enacted but no similar law has been enacted by state Y. Because P's access to D's assets is fundamental to carrying out P's fiduciary duties, a court should apply subsections (b) and (c) of this Act to void the TOSA provision prohibiting P's access to D's online account, even though the TOSA selected the law of state Y to govern the contractual rights and duties under the TOSA.

8. **Section 740.801** addresses compliance.

Subsection (1) allows a fiduciary to request access, control, or a copy of the digital asset. The term "control" means only the ability to move (unless prohibited by copyright law) or delete that particular asset. A fiduciary's control over a digital asset is not equivalent to a transfer of ownership or a laundering of illegally obtained material. Thus, this subsection grants the fiduciary the ability to access electronic records, and the disposition of those records is subject to other laws. For example, where the account holder has an online securities account or has a game character and in-game property associated with an online game, then the fiduciary's ability to sell the securities, the game character, or the in-game property is controlled by traditional probate law. The act is only granting access and "control" in the sense of enabling the fiduciary to do electronically what the account holder could have done electronically. Thus, if a TOSA precludes online transfers, then the fiduciary is unable to make those transfers electronically as well.

Example – Fiduciary control over a digital asset. D dies with a will disposing of all D's assets to D's spouse, S. E is the personal representative for D's estate. D left a bank account, for which D only received online statements, and a blog.

E as personal representative of D's estate has access to both of D's accounts and can request the passwords from the custodians of both accounts. If D's agreement with the bank requires that transferring the underlying title to the account be done in person, through a hard copy signed by the account holder and the bank manager, then E must comply with those procedures (signing as the account holder) and cannot transfer the funds in the account electronically. If the TOSA for the blog permitted D to transfer the blog electronically, then E can make the transfer electronically as well.

Subsection (3) establishes 60 days as the appropriate time for compliance. If applicable law other than this act does not prohibit the custodian from complying, then the custodian must grant access to comply.

9. **Section 740.901** grants immunity to custodians.

This section establishes that custodians are protected from liability when they act in accordance with the procedures of this Act and in good faith. The types of actions covered include disclosure as well as transfer of copies.

10. **Section 740.1001** establishes the relation with the Electronic Signatures in Global and National Commerce Act.

11. **Section 740.1101** establishes the applicability of this Act. This Act applies in situations in which a decedent dies testate or intestate, as well as a guardianship.

This Act does not change the substantive rules of other law, such as agency, banking, guardianship, contract, copyright, criminal, fiduciary, privacy, probate, property, security, trust, or other applicable law except to vest fiduciaries with authority, according to the provisions of this Act, to access, control, or copy digital assets of a decedent, ward, principal, settlor, or trustee.

12. **Section 12** establishes the effective date.

IV. FISCAL IMPACT ON STATE AND LOCAL GOVERNMENTS

The proposal does not have a fiscal impact on state or local governments. In fact, it should decrease the risk of unauthorized access to digital assets from the fiduciaries appointed by account holders and would provide certainty and predictability for courts, account holders, fiduciaries, and Internet service providers.

V. DIRECT ECONOMIC IMPACT ON PRIVATE SECTOR

The proposal does not have a direct economic impact on the private sector.

VI. CONSTITUTIONAL ISSUES

There appear to be no constitutional issues raised by this proposal.

VII. OTHER INTERESTED PARTIES

Criminal Law Section, State law enforcement and state attorney offices who track and enforce privacy and cyber crimes.
Florida Bankers Association
Business Law Section
Trial Lawyers Association

A bill to be entitled

An act relating to false personation; amending s. 817.02, F.S.; clarifying who may be a victim of false personation; providing for victim restitution; providing for orders correcting public records containing false information; providing an effective date.

Be It Enacted by the Legislature of the State of Florida:

Section 1. Section 817.02, Florida Statutes, is amended to read:

817.02 Obtaining property by false personation.—

(1) Whoever falsely personates or represents another person, as defined in s. 1.01, and in such assumed character receives any property intended to be delivered to that person ~~the party so personated~~, with intent to convert the same to his or her own use, shall be punished as if he or she had been convicted of larceny.

(2)(a) In sentencing a defendant convicted of an offense under this section, the court may order that the defendant make restitution under s. 775.089 to a victim of the offense. In addition to the victim's out-of-pocket costs, restitution may include payment of other costs, including attorney fees incurred by the victim in clearing the victim's credit history or credit rating, or costs incurred in connection with a civil or

administrative proceeding to satisfy a debt, lien, or other obligation of the victim arising as the result of the actions of the defendant.

(b) The sentencing court may issue such orders as are necessary to correct a public record that contains false information given in violation of this section.

Section 2. This act shall take effect October 1, 2014.

Business Identity Theft:
The Unknown Risk to Florida Businesses

September 2013

By
Carrie Kerskie

Kerskie Group, Inc.
PO Box 770311
Naples, Florida 34107
(239) 435-9111

INTRODUCTION

Small businesses in Florida are at risk of business identity theft. Everything needed to commit business identity theft is available on the Secretary of State business filing website www.Sunbiz.org. However, business identity theft is NOT a crime, by statute, in Florida.

Business identity theft occurs when someone uses the identifying information (company name, tax ID number, etc) of a business without the consent of the business. Small businesses are the top targets for business identity theft as they typically do not have the resources, such as a legal department and/or IT department, to detect business identity theft.

Business identity theft is easier and more lucrative for criminals. On average individual identity theft may net a criminal less than $5,000 while a business target can generate 10 times that amount or more.[1]

"From a criminal's viewpoint, it's far more cost-effective to target a business than a consumer."
California Deputy Attorney General Robert Morgenter

"What is particularly disturbing about this trend is the significant dollar amounts involved. It's not unusual for the losses to be in the mid-six figures by the time the criminal activity is detected."
Robert Strezze, Sr. Risk Analyst, Dun & Bradstreet[2]

TYPES OF BUSINESS IDENTITY THEFT

The term "business identity theft' is often used to describe the myriad of scenarios involving the fraudulent, or unauthorized, use of a company's identity. Here are a few examples.[3]

-Identity thieves in New York used financial information obtained from corrupt bank employees to cash counterfeit payroll checks that were designed to look like they belonged to the victim organizations, which included corporations, hospitals, and government agencies.[4]

- In California, criminals rented office space in the same building as a legitimate business, ordering corporate credit cards or retail merchandise in the businesses' name, and then disappeared by the time the business realized that its identity has been stolen. [5]

- A Nevada man claimed that the identity of his business was stolen after a company changed the name of the businesses' officers through filings with the Secretary of State's office, then sold the business to a third party.[6]

- In New Jersey, a company accused a former employee of corporate identity theft after the employee posed as the company on various social networking and business-related sites, all the while posting negative information about the company. [7]

- Large companies such as eBay, Microsoft, and VISA, have dealt with business identity theft carried out through "phishing" schemes where fraudulent emails purporting to be from legitimate, recognizable businesses seek personal or financial information from recipients. [8]

- In Tennessee, criminals have been creating phony web sites that impersonate the identity of legitimate car dealerships and advertise low prices in order to scam people into making deposits for vehicles that do not exist. [9]

- In Georgia, criminals purchased a cell phone, registered it under the name of "Georgia Powers" (which showed up on caller ID), and convinced a number of elderly people – who thought they were speaking with the utility company "Georgia Power" – to divulge their credit card data.[10]

CONSEQUENCES OF BUSINESS IDENTITY THEFT

To the business

- Loss of personal income
- Loss of production
- Unable to focus on sales/productivity
- Negative tax consequences
- Personal liability
- Inability to meet payroll, tax obligation or to pay bills
- Business failure

It should be noted that I attempted to contact Florida businesses that were listed in various articles as having been a victim of business identity theft to get their perspective. Unfortunately I was unable to find one that was still in business.

To the State

- Loss of revenue
- Loss of jobs
- Higher unemployment

While it is difficult to determine the actual number of reported cases and the dollar loss to the business and the state Ricky Harper, former director of the Division of Corporations at the Florida Department of State, estimated that as of January 2013 there were "130 cases with accumulated losses of about $6 million." He further stated that the Division of Corporations knows of "maybe 1% of what is actually going on out there." The Florida Department of State Division of Corporations estimates that **60% of businesses that fall victim to business identity theft will fail within one year of the incident.[11]**

GAP IN STATUTES

Even though business identity theft is a real threat and has the potential to affect numerous individuals (owners and employees) it is not an actual crime in numerous states. The majority of the states, with the exception of California, exempt business entities from identity theft statutes. This is also true on the federal level however for purposes of this paper the focus will remain on state statutes.

"*There is a real gap. The current federal laws look at identity theft as a crime against individuals"* stated Betsy Broder, former Assistant Director of the FTC's Divison of Privacy and Identity Protection. [12]

So just how did businesses get left behind in the various state and federal identity theft laws? Unfortunately many states waited until individual identity theft became an epidemic before taking action. The majority of the federal prevention laws in place today were a direct result of the Federal Trade Commission documenting the ever increasing trend of individual identity theft. However, the FTC does not track tends of business identity theft. Even today many states are not diligently tracking business identity theft.

Florida statute 817.568 titled "Criminal use of personal identifying information" states

Any person who willfully and without authorization fraudulently uses, or possesses with intent to fraudulently use, personal identification information ***concerning an individual*** *without first obtaining that individual's consent, commits the offense of fraudulent use of personal identification information, which is a felony of the third degree, punishable as provided in s. 775.082, s. 775.083, or s. 775.084.*

The statute defines an individual as

a single human being and ***does not mean*** *a firm, association of individuals, corporation, partnership, joint venture, sole proprietorship, or any other entity.*

Therefore using the personal identifying information of a business is not a crime. However, as stated earlier, the personal identifying information needed to commit business identity theft is public record and available on the Division of Corporations website, www.sunbiz.org.

There is another Florida statute involving false personation however it is very limited in scope.

817.02 Obtaining property by false personation.—Whoever falsely personates or represents another, and in such assumed character receives any property intended to be delivered to the party so personated, with intent to convert the same to his or her own use, shall be punished as if he or she had been convicted of larceny.

In 2006 California recognized the need for a change in the state law.
"We were having businesses being taken over and their names being used and I could not prosecute them, at least no under identity theft statutes" said California Deputy Attorney General Robert Morgester.

California was the first state to include business entities in the definition of an individual.

530.55. (a) For purposes of this chapter, "person" means a natural person, living or deceased, firm, association, organization,partnership, business trust, company, corporation, limited liability company, or public entity, or any other legal entity.

Businesses are now afforded the same restoration rights as individuals, based on the California Identity Theft law penal code 528-539. This includes, but is not limited to, initiating an investigation with law enforcement, receiving a police report and the right to receive information

It should be noted that I have worked with hundreds of identity theft victims, individual and business, since 2007. With the rights given to individual victims on the state and federal level I am able to, on average, restore the individual's identity within a few hours. However, it can take many months to a few years to attempt to restore a business identity if it is able to be restored before the business closes.

relating to fraudulent applications and/or accounts. Without these rights a business is limited in the restoration of its business identity.

THE SOLUTION

Change the current Florida statute[13] to include business entities as "individuals" or draft a new one based on both the Florida statute and the California penal code.[14] While merely changing the Florida statue definition of "individual" to include a business entity will allow a business to initiate an investigation by law enforcement the statute lacks the restoration rights for business identity theft victims. Currently, under federal laws, individuals are given specific rights to aid in the restoration of their identities. Businesses are exempt from these laws meaning they are not given the same restoration rights.

Right now criminals know that there is a "free pass" on Florida companies and the only recourse a Florida company has is to file a civil suit. If the identity thief is not brought to justice then he is allowed to commit the crime again and again.

Benefits to business
Easier and faster restoration
Save money
Save time
Reduces the risk

Benefits to Florida
Show we are a business friendly state
Proactive on protecting Florida small businesses
Reduce unemployment
Reduce job losses
Increase revenue

CONCLUSION

Florida has more businesses than any other state so statistically Florida is a target for business identity theft. Florida is number one in the country for individual identity theft. Let's not wait until Florida is also number one for business identity theft. The time for action is now.

Endnotes

[1] Tozzi, John "Identity Theft: The Business Bust-Out" July 23, 2007
[2]Link to website
http://www.businessidtheft.org/Education/WhyBusinessIDTheft/tabid/85/Default.aspx
[3] NASS "Developing State Solutions to Business Identity Theft" January 2012
[4] Miller, Chuck. "Identity theft ring busted in New York," *SC Magazine*, May 28, 2009.
[5] Spielberg, Greg T. "Taking On Small-Business Identity Theft," *Bloomberg Businessweek*, July 9, 2009.
[6] Norman, Jan. "Irvine businessman sues over corporate identity theft," *The Orange County Register*, May 21, 2008.
[7] "David Landau & Associates, LLC Uncovers Identity Theft, Corporate Impersonation," *PR Newswire*, Sept. 8, 2011.
[8] Edwards, John. "Preventing Business Identity Theft," *CFO*, May 19, 2004
[9] Ransom, Kevin. "Stolen Dealer Identity Baits Car Shoppers," *AOL Autos*, August 4, 2010.
[10] Rankin, Bill. "Scams more high-tech, vicious," *The Atlanta Journal-Constitution*, May 27, 2011.
[11] Kellian, Mark "Business ID theft of the rise" January 15, 2013
[12] Tozzi, John "Identity Theft: The Business Bust-Out" July 23, 2007
[13] Link to Florida statute 817.568
http://archive.flsenate.gov/statutes/index.cfm?m&App_mode=Display_Statute&Search_String=&URL=0800-0899/0817/Sections/0817.568.html
[14] Link to California penal code 528-239
http://www.leginfo.ca.gov/cgi-bin/displaycode?section=pen&group=00001-01000&file=528-539

Business Identity Theft:
The Unknown Risk to Florida Businesses

September 2013

By
Carrie Kerskie

Kerskie Group, Inc.
PO Box 770311
Naples, Florida 34107
(239) 435-9111

INTRODUCTION

Small businesses in Florida are at risk of business identity theft. Everything needed to commit business identity theft is available on the Secretary of State business filing website www.Sunbiz.org. However, business identity theft is NOT a crime, by statute, in Florida.

Business identity theft occurs when someone uses the identifying information (company name, tax ID number, etc) of a business without the consent of the business. Small businesses are the top targets for business identity theft as they typically do not have the resources, such as a legal department and/or IT department, to detect business identity theft.

Business identity theft is easier and more lucrative for criminals. On average individual identity theft may net a criminal less than $5,000 while a business target can generate 10 times that amount or more.[1]

"From a criminal's viewpoint, it's far more cost-effective to target a business than a consumer."
California Deputy Attorney General Robert Morgenter

"What is particularly disturbing about this trend is the significant dollar amounts involved. It's not unusual for the losses to be in the mid-six figures by the time the criminal activity is detected."
Robert Strezze, Sr. Risk Analyst, Dun & Bradstreet[2]

TYPES OF BUSINESS IDENTITY THEFT

The term "business identity theft' is often used to describe the myriad of scenarios involving the fraudulent, or unauthorized, use of a company's identity. Here are a few examples.[3]

-Identity thieves in New York used financial information obtained from corrupt bank employees to cash counterfeit payroll checks that were designed to look like they belonged to the victim organizations, which included corporations, hospitals, and government agencies.[4]

- In California, criminals rented office space in the same building as a legitimate business, ordering corporate credit cards or retail merchandise in the businesses' name, and then disappeared by the time the business realized that its identity has been stolen. [5]

- A Nevada man claimed that the identity of his business was stolen after a company changed the name of the businesses' officers through filings with the Secretary of State's office, then sold the business to a third party.[6]

- In New Jersey, a company accused a former employee of corporate identity theft after the employee posed as the company on various social networking and business-related sites, all the while posting negative information about the company. [7]

- Large companies such as eBay, Microsoft, and VISA, have dealt with business identity theft carried out through "phishing" schemes where fraudulent emails purporting to be from legitimate, recognizable businesses seek personal or financial information from recipients. [8]

- In Tennessee, criminals have been creating phony web sites that impersonate the identity of legitimate car dealerships and advertise low prices in order to scam people into making deposits for vehicles that do not exist. [9]

- In Georgia, criminals purchased a cell phone, registered it under the name of "Georgia Powers" (which showed up on caller ID), and convinced a number of elderly people – who thought they were speaking with the utility company "Georgia Power" – to divulge their credit card data.[10]

CONSEQUENCES OF BUSINESS IDENTITY THEFT

To the business

- Loss of personal income
- Loss of production
- Unable to focus on sales/productivity
- Negative tax consequences
- Personal liability
- Inability to meet payroll, tax obligation or to pay bills
- Business failure

It should be noted that I attempted to contact Florida businesses that were listed in various articles as having been a victim of business identity theft to get their perspective. Unfortunately I was unable to find one that was still in business.

To the State

- Loss of revenue
- Loss of jobs
- Higher unemployment

While it is difficult to determine the actual number of reported cases and the dollar loss to the business and the state Ricky Harper, former director of the Division of Corporations at the Florida Department of State, estimated that as of January 2013 there were "130 cases with accumulated losses of about $6 million." He further stated that the Division of Corporations knows of "maybe 1% of what is actually going on out there." The Florida Department of State Division of Corporations estimates that **60% of businesses that fall victim to business identity theft will fail within one year of the incident.[11]**

GAP IN STATUTES

Even though business identity theft is a real threat and has the potential to affect numerous individuals (owners and employees) it is not an actual crime in numerous states. The majority of the states, with the exception of California, exempt business entities from identity theft statutes. This is also true on the federal level however for purposes of this paper the focus will remain on state statutes.

"*There is a real gap. The current federal laws look at identity theft as a crime against individuals"* stated Betsy Broder, former Assistant Director of the FTC's Divison of Privacy and Identity Protection. [12]

So just how did businesses get left behind in the various state and federal identity theft laws? Unfortunately many states waited until individual identity theft became an epidemic before taking action. The majority of the federal prevention laws in place today were a direct result of the Federal Trade Commission documenting the ever increasing trend of individual identity theft. However, the FTC does not track tends of business identity theft. Even today many states are not diligently tracking business identity theft.

Florida statute 817.568 titled "Criminal use of personal identifying information" states

Any person who willfully and without authorization fraudulently uses, or possesses with intent to fraudulently use, personal identification information ***concerning an individual*** *without first obtaining that individual's consent, commits the offense of fraudulent use of personal identification information, which is a felony of the third degree, punishable as provided in s. 775.082, s. 775.083, or s. 775.084.*

The statute defines an individual as

a single human being and ***does not mean*** *a firm, association of individuals, corporation, partnership, joint venture, sole proprietorship, or any other entity.*

Therefore using the personal identifying information of a business is not a crime. However, as stated earlier, the personal identifying information needed to commit business identity theft is public record and available on the Division of Corporations website, www.sunbiz.org.

There is another Florida statute involving false personation however it is very limited in scope.

817.02 Obtaining property by false personation.—Whoever falsely personates or represents another, and in such assumed character receives any property intended to be delivered to the party so personated, with intent to convert the same to his or her own use, shall be punished as if he or she had been convicted of larceny.

In 2006 California recognized the need for a change in the state law.
"We were having businesses being taken over and their names being used and I could not prosecute them, at least no under identity theft statutes" said California Deputy Attorney General Robert Morgester.

California was the first state to include business entities in the definition of an individual.

530.55. (a) For purposes of this chapter, "person" means a natural person, living or deceased, firm, association, organization,partnership, business trust, company, corporation, limited liability company, or public entity, or any other legal entity.

Businesses are now afforded the same restoration rights as individuals, based on the California Identity Theft law penal code 528-539. This includes, but is not limited to, initiating an investigation with law enforcement, receiving a police report and the right to receive information

It should be noted that I have worked with hundreds of identity theft victims, individual and business, since 2007. With the rights given to individual victims on the state and federal level I am able to, on average, restore the individual's identity within a few hours. However, it can take many months to a few years to attempt to restore a business identity if it is able to be restored before the business closes.

relating to fraudulent applications and/or accounts. Without these rights a business is limited in the restoration of its business identity.

THE SOLUTION

Change the current Florida statute[13] to include business entities as "individuals" or draft a new one based on both the Florida statute and the California penal code.[14] While merely changing the Florida statue definition of "individual" to include a business entity will allow a business to initiate an investigation by law enforcement the statute lacks the restoration rights for business identity theft victims. Currently, under federal laws, individuals are given specific rights to aid in the restoration of their identities. Businesses are exempt from these laws meaning they are not given the same restoration rights.

Right now criminals know that there is a "free pass" on Florida companies and the only recourse a Florida company has is to file a civil suit. If the identity thief is not brought to justice then he is allowed to commit the crime again and again.

Benefits to business
Easier and faster restoration
Save money
Save time
Reduces the risk

Benefits to Florida
Show we are a business friendly state
Proactive on protecting Florida small businesses
Reduce unemployment
Reduce job losses
Increase revenue

CONCLUSION

Florida has more businesses than any other state so statistically Florida is a target for business identity theft. Florida is number one in the country for individual identity theft. Let's not wait until Florida is also number one for business identity theft. The time for action is now.

Endnotes

[1] Tozzi, John "Identity Theft: The Business Bust-Out" July 23, 2007
[2]Link to website
http://www.businessidtheft.org/Education/WhyBusinessIDTheft/tabid/85/Default.aspx
[3] NASS "Developing State Solutions to Business Identity Theft" January 2012
[4] Miller, Chuck. "Identity theft ring busted in New York," *SC Magazine*, May 28, 2009.
[5] Spielberg, Greg T. "Taking On Small-Business Identity Theft," *Bloomberg Businessweek*, July 9, 2009.
[6] Norman, Jan. "Irvine businessman sues over corporate identity theft," *The Orange County Register*, May 21, 2008.
[7] "David Landau & Associates, LLC Uncovers Identity Theft, Corporate Impersonation," *PR Newswire*, Sept. 8, 2011.
[8] Edwards, John. "Preventing Business Identity Theft," *CFO*, May 19, 2004
[9] Ransom, Kevin. "Stolen Dealer Identity Baits Car Shoppers," *AOL Autos*, August 4, 2010.
[10] Rankin, Bill. "Scams more high-tech, vicious," *The Atlanta Journal-Constitution*, May 27, 2011.
[11] Kellian, Mark "Business ID theft of the rise" January 15, 2013
[12] Tozzi, John "Identity Theft: The Business Bust-Out" July 23, 2007
[13] Link to Florida statute 817.568
http://archive.flsenate.gov/statutes/index.cfm?m&App_mode=Display_Statute&Search_String=&URL=0800-0899/0817/Sections/0817.568.html
[14] Link to California penal code 528-239
http://www.leginfo.ca.gov/cgi-bin/displaycode?section=pen&group=00001-01000&file=528-539

A bill to be entitled

An act relating to financial literacy instruction in the public schools; amending s. 1003.41, F.S.; revising Next Generation Sunshine State Standards for financial literacy instruction; requiring the Department of Education to work with nonprofit organizations to develop standards and curriculum for financial literacy instruction; deleting an obsolete requirement relating to a cost analysis for implementing a separate course in financial literacy; amending s. 1003.4282, F.S.; providing that credit requirements for high school graduation and a standard diploma include a separate course in financial literacy; revising credit requirements to conform; amending s. 1012.98, F.S.; requiring the department to work with nonprofit organizations to provide guidelines and resources for professional development for teaching financial literacy; requiring specified professional development; providing an effective date.

Be It Enacted by the Legislature of the State of Florida:

Section 1. Paragraph (d) of subsection (2) and subsection (3) of section 1003.41, Florida Statutes, are amended to read:

1003.41 Next Generation Sunshine State Standards.—

(2) Next Generation Sunshine State Standards must meet the

following requirements:

(d) Social Studies standards must establish specific curricular content for, at a minimum, geography, United States and world history, government, civics, humanities, ~~and~~ economics, and ~~including~~ financial literacy. Financial literacy includes the knowledge, understanding, skills, behaviors, attitudes, and values that will enable a student to make responsible and effective financial decisions on a daily basis. Financial literacy instruction shall ~~be an integral part of instruction throughout the entire economics course and~~ include information regarding earning income; buying goods and services; saving and financial investing, including an understanding of compound interest; decisionmaking through weighing costs and benefits; insurance; taxes; the use of credit and credit cards, including an understanding of interest and online commerce; budgeting and debt management, including student loans and secured loans; banking and financial services; planning for one's financial future, including higher education and career planning; credit reports and scores; and fraud and identity theft prevention. The Department of Education shall work with nonprofit organizations with proven expertise in the development of standards and curriculum for financial literacy instruction.

(3) The Commissioner of Education, as needed, shall develop and submit proposed revisions to the standards for review and comment by Florida educators, school administrators, representatives of the Florida College System institutions and

state universities who have expertise in the content knowledge and skills necessary to prepare a student for postsecondary education and careers, business and industry leaders, and the public. The commissioner, after considering reviews and comments, shall submit the proposed revisions to the State Board of Education for adoption. ~~In addition, the commissioner shall prepare an analysis of the costs associated with implementing a separate, one-half credit course in financial literacy, including estimated costs for instructional personnel, training, and the development or purchase of instructional materials. The commissioner shall work with one or more nonprofit organizations with proven expertise in the area of personal finance, consider free resources that can be utilized for instructional materials, and provide data on the implementation of such a course in other states. The commissioner shall provide the cost analysis to the President of the Senate and the Speaker of the House of Representatives by October 1, 2013.~~

Section 2. Paragraphs (d) and (g) of subsection (3) of section 1003.4282, Florida Statutes, are amended to read:

1003.4282 Requirements for a standard high school diploma.—

(3) STANDARD HIGH SCHOOL DIPLOMA; COURSE AND ASSESSMENT REQUIREMENTS.—

(d) Three credits in social studies.—A student must earn one credit in United States History; one credit in World History; one-half credit in economics, which must include

financial literacy; and one-half credit in United States Government. The United States History EOC assessment constitutes 30 percent of the student's final course grade. Beginning with students entering grade 9 in the 2014-2015 school year, a student must earn three and one-half credits in social studies, which includes one credit in United States History, one credit in World History, one-half credit in economics, one-half credit in financial literacy, and one-half credit in United States Government.

(g) Eight credits in electives or, beginning with students entering grade 9 in the 2014-2015 school year, seven and one-half credits in electives.—School districts must develop and offer coordinated electives so that a student may develop knowledge and skills in his or her area of interest, such as electives with a STEM or liberal arts focus. Such electives must include opportunities for students to earn college credit, including industry-certified career education programs or series of career-themed courses that result in industry certification or articulate into the award of college credit, or career education courses for which there is a statewide or local articulation agreement and which lead to college credit.

Section 3. Subsection (13) is added to section 1012.98, Florida Statutes, to read:

1012.98 School Community Professional Development Act.—

(13) The department shall work with one or more nonprofit organizations with proven expertise in the delivery of teacher

professional development in financial literacy instruction for the purpose of providing guidelines, materials, resources, and professional development activities. Instructional personnel who are not certified in social studies, economics, business, or marketing must complete a minimum of 14 hours of professional development in financial literacy before teaching a high school course in financial literacy.

Section 4. This act shall take effect July 1, 2014.

Be It Enacted by the Legislature of the State of Florida:

Section 1. Subsection (37) of Section 605.0102 is amended to read:

605.0102 Definitions.—As used in this chapter, the term:

(37) "Majority-in-interest" means those members who hold more than 50 percent of the then-current percentage or other interest in the profits of the limited liability company ~~and who have the right to vote~~ owned by all of its members; however, as used in ss. 605.1001¬605.1072, the term means:

(a) In the case of a limited liability company with only one class or series of members, the holders of more than 50 percent of the then-current percentage or other interest in the profits of the company owned by all of its members who have the right to approve ~~a~~ the merger, interest exchange, or conversion, as applicable, under the organic law or the organic rules of the company; and

(b) In the case of a limited liability company having more than one class or series of members, the holders in each class or series of more than 50 percent of the then-current percentage or other interest in the profits of the company owned by all of the members of that class or series who have the right to approve ~~a~~ the merger, interest exchange, or conversion, as applicable, under the organic law or the organic rules of the company, unless the company's organic rules provide for the approval of the transaction in a different manner.

(b) In the case of a limited liability company having more

Section 2. Subsection (4)(b)5. of Section 605.0103 is amended to read:

CODING: Words ~~stricken~~ are deletions; words underlined are additions.

V

605.0103 Knowledge; notice.—

5. Grant of authority to or limitation imposed on the authority of a person holding a position or having a specified status in a company, or grant of authority to or limitation imposed on the authority of a specific person, if the grant of authority or limitation imposed on the authority is described in the articles of organization in accordance with s. 605.0201(3)(d); however, if that description has been added or changed by an amendment or an amendment and restatement of the articles of organization, notice of the addition or change may not become effective until 90 days after the effective date of such amendment or amendment and restatement. A provision in the articles of organization limiting the authority of a person to transfer real property held in the name of the limited liability company is not notice of the limitation to a person who is not a member or manager of the company, unless the limitation appears in an affidavit, certificate, or other instrument that bears the name of the limited liability company and is recorded in the office for recording transfers of such real property.

Section 3. Subsection (4) of Section 605.04073 is amended to read:

605.04073 Voting rights of members and managers.—

(4) An action requiring the vote or consent of members under this chapter may be taken without a meeting, if the action is approved in a record by the members having not less than the minimum number of votes that would be necessary to authorize or take the action at a meeting of the members. ~~and a~~ A member may appoint a proxy or other agent to vote or consent for the member by signing an appointing record, personally or by the member's agent. On an action taken by fewer than all of the

V

members without a meeting, notice of the action must be given to those members who did not consent in writing to the action or who were not entitled to vote on the action within 10 days after the action was taken.

Section 4. Subsection (4)(b) of Section 605.0408 is amended to read:

605.0408 Reimbursement, indemnification, advancement, and insurance.—

(b) Under s. 605.0105(3)~~(p)~~(q) the operating agreement could not provide for indemnification for the conduct giving rise to the liability.

Section 6. Subsection (2)(b) of Section 605.04091 is amended to read:

605.04091 Standards of conduct for members and managers.—

(b) Refraining from dealing with the company in the conduct or winding up of the company's activities and affairs as, or on behalf of, a person having an interest adverse to the company, except to the extent that a transaction satisfies the requirements of ~~this~~ section 605.04092; and

Section 7. Subsection (2) of Section 605.0410 is amended to read:

605.0410 Records to be kept; rights of member, manager, and person dissociated to information.-

(2) In a member-managed limited liability company, the following rules apply:

(a) Upon reasonable notice, a member may inspect and copy during regular business hours, at a reasonable location specified by the company:

1. The records described in subsection (1); and

2. Each other record maintained by the company regarding

V

the company's activities, affairs, financial condition, and other circumstances, to the extent the information is material to the member's rights and duties under the operating agreement or this chapter.

(b) The company shall furnish to each member:

1. Without demand, any information concerning the company's activities, affairs, financial condition, and other circumstances that the company knows and are material to the proper exercise of the member's rights and duties under the operating agreement or this chapter, except to the extent the company can establish that it reasonably believes the member already knows the information; and

2. On demand, other information concerning the company's activities, affairs, financial condition, and other circumstances, except to the extent the demand or information demanded is unreasonable or otherwise improper under the circumstances.

(c) Within 10 days after receiving a demand pursuant to subparagraph (2)(b)2., the company shall, in a record, inform the member who made the demand of:

1. The information that the company will provide in response to the demand and when and where the company will provide the information; and

2. The company's reasons for declining, if the company declines to provide any demanded information.

~~(c)~~ (d) The duty to furnish information under this subsection also applies to each member to the extent the member knows any of the information described in this subsection.

Section 8. Subsection (3)(c) of Section 605.0410 is amended to read:

605.0410 Records to be kept; rights of member, manager, and person dissociated to information.-

(c) Within 10 days after receiving a demand pursuant to subparagraph ~~(2)~~ (3)(b)2., the company shall, in a record, inform the member who made the demand of:

1. The information that the company will provide in response to the demand and when and where the company will provide the information; and

2. The company's reasons for declining, if the company declines to provide any demanded information.

Section 9. Subsection (4) of Section 605.0410 is amended to read:

605.0410 Records to be kept; rights of member, manager, and person dissociated to information.-

(4) Subject to subsection ~~(9)~~ (10), on 10 days' demand made in a record received by a limited liability company, a person dissociated as a member may have access to information to which the person was entitled while a member if:

Section 10. Subsection (2)(f) of Section 605.1025 is amended to read:

605.1025 Articles of merger.—

(f) If the surviving entity is created by the merger and is a domestic limited liability partnership ~~or domestic limited liability limited partnership~~, its statement of qualification, as an attachment.

Section 11. Subsection (3) of Section 605.1108 is amended to read:

605.1108 Application to limited liability company formed under the Florida Limited Liability Company Act.—

(3) For the purpose of applying this chapter to a limited

V

liability company formed before January 1, 2014, under the Florida Limited Liability Company Act, ss. 608.401-608.705~~:~~ ~~(a) T~~ , the company's articles of organization are deemed to be the company's articles of organization under this chapter.~~;~~ ~~and~~

~~(b) For the purpose of applying s. 605.0102(39), the language in the company's articles of organization designating the company's management structure operates as if that language were in the operating agreement.~~

Section 12. Subsection (3) of Section 605.1041 is amended to read:

605.1041 Conversion authorized.—

(3) By complying with the provisions of ss. 605.1041¬605.1046 ~~608.1046~~ which are applicable to foreign entities, a foreign entity may become a domestic limited liability company if the conversion is authorized by the law of the foreign entity's jurisdiction of formation.

Section 13. [This act][The amendments in Sections _____ through _____ above] shall take effect January 1, 2014.

V

CODING: Words ~~stricken~~ are deletions; words underlined are additions.

V

PROCEEDINGS SUPPLEMENTARY TASK FORCE
July 21, 2014
REVISED ISSUES

1. Whether the threshold procedure for instituting proceedings supplementary is sufficient.

2. Whether the statutory procedure is sufficient for a court to determine whether to summon a non-party.

3. Jurisdiction and venue considerations.

4. When can a court issue process to attach property?

5. Whether a non-party should be entitled to a jury trial.

6. Whether an impleaded defendant may be held liable for attorney's fees and damages in addition to turning over the debtor's property.

7. Whether superpriority over pre-existing judgment liens is appropriate.

8. Whether the statute should explicitly define types of assets recoverable through proceedings supplementary.

9. Whether a court in a proceeding supplementary may compel an entity the court has personal jurisdiction over to turn over property located outside the jurisdiction which is in the possession or control of that entity.

10. Whether the amendment's inclusion of Chapter 726 claims merits a further amendment to make clear that proceedings supplementary are part of or ancillary to the original lawsuit

An act relating to the court system; repealing s. 25.151, F.S., relating to a prohibition on the practice of law by a retired justice of the Supreme Court; repealing ss. 25.191 and 25.231, F.S., relating to the appointment and duties of a Clerk of the Supreme Court; amending s. 25.241, F.S.; deleting a requirement regarding the salary of the Clerk of the Supreme Court, to conform; repealing s. 25.281, F.S., relating to compensation of the Marshal of the Supreme Court; repealing s. 25.351, F.S., relating to the acquisition of books by the Supreme Court; repealing s. 26.01, F.S., relating to the number of judicial circuits; amending s. 26.021, F.S.; specifying the number of judicial circuits; repealing certain residency requirements for circuit judges; repealing s. 26.51, F.S., relating to payment of the salaries of circuit judges; amending s. 26.55, F.S.; excluding retired judges practicing law from the Conference of Circuit Judges of Florida; removing a requirement that circuit court judges attend and participate in such conference; requiring that the conference operate according to the Rules of Judicial Administration; revising requirements for such conferences; repealing s. 27.55, F.S., relating to compensation and certain expenditures of public defenders; creating s. 29.23, F.S.; providing for certain judicial branch salaries; repealing ss. 35.12, 35.13, 35.19, and 35.21, F.S., relating to the chief judge, quorum, compensation of

judges, and clerk, respectively, of the district courts of appeal; amending s. 35.22, F.S.; deleting a requirement for the appointment and salary of a clerk for each district court of appeal; repealing ss. 35.25 and 35.27, F.S., relating to duties of the clerk and compensation of the marshal, respectively, of the district courts of appeal; repealing s. 38.13, F.S., relating to replacement of disqualified judges of the district courts of appeal; amending s. 43.20, F.S.; revising the number of members of the Judicial Qualifications Commission to conform to requirements of the State Constitution; amending s. 56.29, F.S.; authorizing the court to order any property, debt, or other obligation due the judgment debtor to be applied toward the satisfaction of the judgment debt; authorizing the court to entertain specified claims concerning the judgment debtor's assets and enter any order or judgment, including a money judgment; authorizing the court to enter a money judgment against an impleaded defendant under certain circumstances; providing applicability of specified laws and procedures; providing for retroactivity; repealing s. 57.101, F.S., relating to the charging of costs against the losing party for certain copies of records in the Supreme Court; repealing s. 92.15, F.S., relating to an evidentiary rule regarding evidence of title to land passing from the United States; providing an effective date.

Be It Enacted by the Legislature of the State of Florida:

Section 1. Section 25.151, Florida Statutes, is repealed.

Section 2. Sections 25.191 and 25.231, Florida Statutes, are repealed.

Section 3. Subsection (1) of section 25.241, Florida Statutes, is amended to read:

25.241 Clerk of Supreme Court; compensation; assistants; filing fees, etc.—

~~(1) The Clerk of the Supreme Court shall be paid an annual salary to be determined in accordance with s. 25.382.~~

Section 4. Section 25.281, Florida Statutes, is repealed.

Section 5. Section 25.351, Florida Statutes, is repealed.

Section 6. Section 26.01, Florida Statutes, is repealed.

Section 7. Section 26.021, Florida Statutes, is amended to read:

26.021 Judicial circuits; judges.—The state is divided into 20 judicial circuits:

(1) The first circuit is composed of Escambia, Okaloosa, Santa Rosa, and Walton Counties.

(2) The second circuit is composed of Franklin ~~Leon~~, Gadsden, Jefferson, Leon, Liberty, and Wakulla~~, Liberty, and Franklin~~ Counties.

(3) The third circuit is composed of Columbia, Dixie, Hamilton, Lafayette, Madison, Suwannee, and Taylor Counties.

(4) The fourth circuit is composed of Clay, Duval, and Nassau Counties.

(5) The fifth circuit is composed of Citrus, Hernando, Lake, Marion, and Sumter Counties. ~~Two of the circuit judges~~

~~authorized for the fifth circuit shall reside in either Citrus, Hernando, or Sumter County, and neither of such two judges shall reside in the same county.~~

(6) The sixth circuit is composed of Pasco and Pinellas Counties.

(7) The seventh circuit is composed of Flagler, Putnam, St. Johns, and Volusia Counties. ~~One judge shall reside in Flagler County; two judges shall reside in Putnam County; two judges shall reside in St. Johns County; and three judges shall reside in Volusia County. There shall be no residency requirement for any other judges in the circuit.~~

(8) The eighth circuit is composed of Alachua, Baker, Bradford, Gilchrist, Levy, and Union Counties.

(9) The ninth circuit is composed of Orange and Osceola Counties.

(10) The tenth circuit is composed of Hardee, Highlands, and Polk Counties.

(11) The eleventh circuit is composed of Miami-Dade County.

(12) The twelfth circuit is composed of DeSoto, Manatee, and Sarasota~~, and DeSoto~~ Counties.

(13) The thirteenth circuit is composed of Hillsborough County.

(14) The fourteenth circuit is composed of Bay, Calhoun, Gulf, Holmes, Jackson, and Washington Counties.

(15) The fifteenth circuit is composed of Palm Beach County.

(16) The sixteenth circuit is composed of Monroe County. ~~One judge in the circuit shall reside in the middle or upper Keys. There shall be no residency requirement for any other~~

~~judge in the circuit.~~

(17) The seventeenth circuit is composed of Broward County.

(18) The eighteenth circuit is composed of Brevard and Seminole Counties.

(19) The nineteenth circuit is composed of Indian River, Martin, Okeechobee, and St. Lucie Counties.

(20) The twentieth circuit is composed of Charlotte, Collier, Glades, Hendry, and Lee Counties.

(21) Notwithstanding subsections (1)-(20), the territorial jurisdiction of a circuit court may be expanded as provided for in s. 910.03(3).

The judicial nominating commission of each circuit, in submitting nominations for any vacancy in a judgeship, and the Governor, in filling any vacancy for a judgeship, shall consider whether the existing judges within the circuit, together with potential nominees or appointees, reflect the geographic distribution of the population within the circuit, the geographic distribution of the caseload within the circuit, the racial and ethnic diversity of the population within the circuit, and the geographic distribution of the racial and ethnic minority population within the circuit.

Section 8. Section 26.51, Florida Statutes, is repealed.

Section 9. Section 26.55, Florida Statutes, is amended to read:

26.55 Conference of Circuit Judges of Florida; duties and reports.—

(1) There is created and established the Conference of Circuit Judges of Florida. The conference consists ~~shall consist~~

of the active and retired circuit judges of the several judicial circuits of the state, excluding retired judges practicing law.

(2) The conference shall annually elect a chair. The chair~~, whose duty it~~ shall ~~be to~~ call all meetings and ~~to~~ appoint committees to effectuate the purposes of the conference. ~~It is declared to be an official function of each circuit judge to attend the meetings of the conference. It is also an official function of each circuit judge to participate in the activity of each committee to the membership of which such judge is appointed.~~

(3)~~(a) It is declared to be the responsibility of~~ The conference shall operate according to the Rules of Judicial Administration adopted by the Supreme Court. The responsibilities of the conference include ~~to~~:

(a)~~1.~~ Considering and making ~~Consider and make~~ recommendations concerning the betterment of the judicial system of the state and its various parts;

(b)~~2.~~ Considering and making ~~Consider and make~~ recommendations concerning the improvement of rules and methods of procedure and practice in the several courts; ~~and~~

(c)~~3.~~ Reporting ~~Report~~ to the Supreme Court its ~~such~~ findings and recommendations under this subsection; and ~~as the conference may have with reference thereto.~~

(d)~~(b)~~ Providing ~~Not less than 60 days before the convening of the regular session of~~ the Legislature with~~, the chair of the conference shall report to the President of the Senate and the Speaker of the House~~ such recommendations as the conference may have concerning defects in the laws of this state and such amendments or additional legislation as the conference may deem

necessary regarding the administration of justice.

Section 10. Section 27.55, Florida Statutes, is repealed.

Section 11. Section 29.23, Florida Statutes, is created to read:

29.23 Salaries of certain positions in the judicial branch.—

(1) The salaries of justices, judges of the district courts of appeal, circuit judges, and county judges shall be fixed annually in the General Appropriations Act.

(2) The clerk and the marshal of the Supreme Court, or a clerk or marshal of a district court of appeal, shall be paid an annual salary to be determined in accordance with s. 25.382(3).

Section 12. Sections 35.12, 35.13, 35.19, and 35.21, Florida Statutes, are repealed.

Section 13. Section 35.22, Florida Statutes, is amended to read:

35.22 Clerk of district court; ~~appointment;~~ compensation; assistants; filing fees; teleconferencing.—

~~(1) Each district court of appeal shall appoint a clerk who shall be paid an annual salary to be determined in accordance with s. 25.382.~~

(1)~~(2)~~ The clerk may ~~is authorized to~~ employ ~~such~~ deputies and clerical assistants as may be necessary. Their number and compensation shall be approved by the court, and paid from the annual appropriation for the district courts of appeal.

(2)~~(3)~~(a) The clerk, upon the filing of a certified copy of a notice of appeal or petition, shall charge and collect a filing fee of $300 for each case docketed, and service charges as provided in s. 28.24 for copying, certifying or furnishing

opinions, records, papers or other instruments and for other services. The state ~~of Florida~~ or its agencies, when appearing as appellant or petitioner, is exempt from the filing fee required in this subsection. ~~From each attorney appearance pro hac vice,~~ The clerk shall collect from each attorney appearance pro hac vice a fee of $100 for deposit as provided in this section.

(b) Upon the filing of a notice of cross-appeal, or a notice of joinder or motion to intervene as an appellant, cross-appellant, or petitioner, the clerk shall charge and collect a filing fee of $295. The clerk shall remit the fee to the Department of Revenue for deposit into the General Revenue Fund. The state and its agencies are exempt from the filing fee required by this paragraph.

(3) ~~(4)~~ The opinions of the district court of appeal may ~~shall~~ not be recorded, but the original as filed shall be preserved with the record in each case.

(4) ~~(5)~~ The clerk may ~~is authorized~~ immediately, after a case is disposed of, ~~to~~ supply the judge who tried the case and from whose order, judgment, or decree, appeal or other review is taken, a copy of all opinions, orders, or judgments filed in such case. Copies of opinions, orders, and decrees shall be furnished in all cases to each attorney of record and for publication in Florida reports to the authorized publisher without charge, and copies furnished to other law book publishers at one-half the regular statutory fee.

(5) ~~(6)~~ The clerk of each district court of appeal shall ~~is required to~~ deposit all fees collected in the State Treasury to the credit of the General Revenue Fund, except that $50 of each

$300 filing fee collected shall be deposited into the State Courts Revenue Trust Fund to fund court operations as authorized in the General Appropriations Act. The clerk shall retain an accounting of each such remittance.

(6)~~(7)~~ The clerk of the district court of appeal may ~~is authorized to~~ collect a fee from the parties to an appeal reflecting the actual cost of conducting the proceeding through teleconferencing if ~~where~~ the parties have requested that an oral argument or mediation be conducted through teleconferencing. The fee collected for this purpose shall be used to offset the expenses associated with scheduling the teleconference and shall be deposited in the State Courts Revenue Trust Fund.

Section 14. Sections 35.25 and 35.27, Florida Statutes, are repealed.

Section 15. Section 38.13, Florida Statutes, is repealed.

Section 16. Subsection (2) of section 43.20, Florida Statutes, is amended to read:

43.20 Judicial Qualifications Commission.—

(2) MEMBERSHIP; TERMS.—The commission shall consist of 15 ~~13~~ members. The members of the commission shall serve for terms of 6 years.

Section 17. Subsections (1) and (5), paragraph (b) of subsection (6), and subsection (9) of section 56.29, Florida Statutes, are amended to read:

56.29 Proceedings supplementary.—

(1) When any person or entity holds an unsatisfied judgment or judgment lien obtained under chapter 55, the judgment holder or judgment lienholder may file a motion and an affidavit so

stating, identifying, if applicable, the issuing court, the case number, and the unsatisfied amount of the judgment or judgment lien, including accrued costs and interest, and stating that the execution is valid and outstanding, and thereupon the judgment holder or judgment lienholder is entitled to these proceedings supplementary to execution.

(5) The court ~~judge~~ may order any property of the judgment debtor, not exempt from execution, in the hands of any person, or any property, debt, or other obligation due to the judgment debtor, to be applied toward the satisfaction of the judgment debt. The court may entertain claims concerning the judgment debtor's assets brought under chapter 726 and enter any order or judgment, including a money judgment against any initial or subsequent transferee, in connection therewith, irrespective of whether the transferee has retained the property. Claims under chapter 726 are subject to the provisions of chapter 726 and applicable rules of civil procedure.

(6)

(b) When any gift, transfer, assignment or other conveyance of personal property has been made or contrived by the judgment debtor ~~defendant~~ to delay, hinder or defraud creditors, the court shall order the gift, transfer, assignment or other conveyance to be void and direct the sheriff to take the property to satisfy the execution. This does not authorize seizure of property exempted from levy and sale under execution or property which has passed to a bona fide purchaser for value and without notice. Any person aggrieved by the levy may proceed under ss. 56.16-56.20.

(9) The court may enter any orders, judgments, or writs

required to carry out the purpose of this section, including those orders necessary or proper to subject property or property rights of any judgment debtor ~~defendant~~ to execution, and including entry of money judgments against any impleaded defendant irrespective of whether such defendant has retained the property, subject to ss. 56.18 and 56.19 and applicable principles of equity, and in accordance with chapters 76 and 77 and applicable rules of civil procedure.

Section 18. The amendments made by this act to s. 56.29, Florida Statutes, are remedial in nature, are intended to clarify existing law, and shall be applied retroactively to the full extent permitted by law.

Section 19. Section 57.101, Florida Statutes, is repealed.

Section 20. Section 92.15, Florida Statutes, is repealed.

Section 21. This act shall take effect July 1, 2014.