



Record Retention & Disposal

Put It in Writing

Presented by:

LEGAL EDUCATION DEPARTMENT

of

Attorneys' Title Fund Services, LLC

Unless otherwise noted, all original material
is
Copyright © 2024
by
Attorneys' Title Fund Services, LLC
(800) 336-3863

Please contact the Education Registrar at
(888) 407-7775 regarding this seminar or to
register for any other Fund seminars

All references herein to title insurance policy forms and endorsements are intended to refer to the policy forms and endorsements issued by Fund members as duly appointed title agents of Old Republic National Title Insurance Company.

These materials are for educational use in Fund seminars. They should not be relied on without first considering the law and facts of a matter. Legal documents for others can only be prepared by an attorney after consultation with the client.

Table of Contents		Page Number
1.	PowerPoint	5
2.	R. Regul. FL. Bar 4-1.6	26
3.	16 C.F.R. Pt. 314 – Safeguarding Standards	32
4.	FL Administrative Code 69J-128.030	47
5.	Fund Concept Article: ALTA Best Practice Pillar No. 3	48
6.	R. Regul. FL. Bar 5-1.2	49
7.	R. Regul. FL. Bar 5-1.1	54
8.	FL Statutes 627.7845	58
9.	Old Republic Agency Agreement	59
10.	12 C.F.R. 1024.10	60
11.	12 C.F.R. 1026.25	61
12.	26 C.F.R. 1.1445-2	63
13.	26 C.F.R. 1.6045-4	67
14.	Sample File Closing Checklist	68
15.	Dowda & Fields v. Cobb	69
16.	FL Bar Ethics Opinion 81-8	73

17.	FL Bar Ethics Opinion 63-3	75
18.	FL Bar Ethics Opinion 71-62	76
19.	FL Bar Ethics Opinion 10-2	78
20.	Sample Privacy and Information Security Policy	82
21.	Sample File Retention & Destruction Policy	85
22.	Sample Acknowledgement & Consent	88
23.	Sample Closed File Archive & Destruction Notice	89
24.	Sample Electronic File Policy	90
25.	“You’ve Been Hacked” Concept Article	92
26.	Accreditation Information	96



Record Retention & Disposal

Put It in Writing

Kara Scott
Legal Education Attorney

2

Introduction

- Why? (Ethical)
- What and for how long? (Legal)
- How? (Practical)
- What next? (Written policies)



3

Why? (Ethical)



The Fund

4

Why?

We are responsible to safeguard a client's confidential information to prevent inadvertent or unauthorized disclosure. R. Reg. Fla. Bar 4-1.6(e)

Informed consent must be obtained to reveal confidential information. R. Reg. Fla. Bar 4-1.6(a)

26 The Fund

5

Why?

Information privacy – establish an Information Security Program

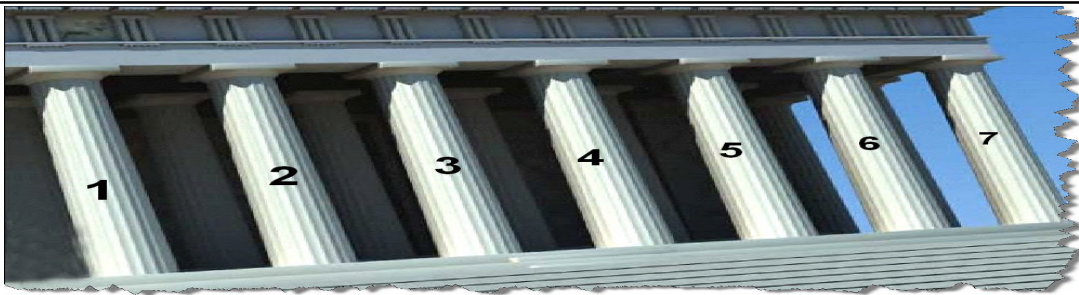


- Gramm-Leach-Bliley Act (GLBA)
 - Safeguards Rule (16 C.F.R. Pt. 314)
- Florida's Safeguards Rule (69J-128.030 et seq. F.A.C.)



The Fund

6



PILLAR 3 – PRIVACY & INFORMATION SECURITY

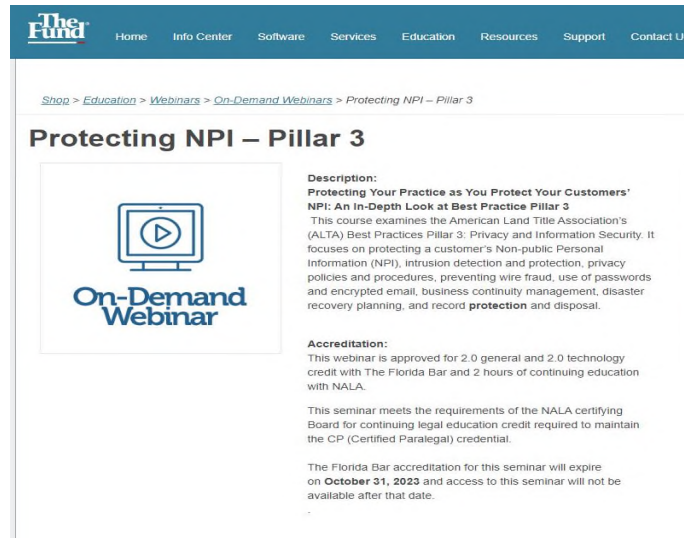
“Adopt and maintain a written privacy and information security program to protect Non-public Personal Information as required by local, state and federal law.”



7

Fund Webinar

Protecting NPI – Pillar 3



The screenshot shows the website for 'The Fund'. The navigation bar includes links for Home, Info Center, Software, Services, Education, Resources, Support, and Contact Us. The breadcrumb trail reads: Shop > Education > Webinars > On-Demand Webinars > Protecting NPI – Pillar 3. The main heading is 'Protecting NPI – Pillar 3'. Below this is a video player icon with the text 'On-Demand Webinar'. To the right, the 'Description' states: 'Protecting Your Practice as You Protect Your Customers' NPI: An In-Depth Look at Best Practice Pillar 3'. It explains that the course examines the American Land Title Association's (ALTA) Best Practices Pillar 3: Privacy and Information Security, focusing on protecting a customer's Non-public Personal Information (NPI), intrusion detection and protection, privacy policies and procedures, preventing wire fraud, use of passwords and encrypted email, business continuity management, disaster recovery planning, and record protection and disposal. The 'Accreditation' section notes that the webinar is approved for 2.0 general and 2.0 technology credit with The Florida Bar and 2 hours of continuing education with NALA. It also states that the seminar meets the requirements of the NALA certifying Board for continuing legal education credit required to maintain the CP (Certified Paralegal) credential. A final note mentions that the Florida Bar accreditation for this seminar will expire on October 31, 2023, and access will not be available after that date. The 'The Fund' logo is in the bottom right corner.

8

Why?



Title Transactions – Trust Accounts R. Reg. Fla. Bar 5-1.2(d)

- Monthly reconciliation
- Monthly comparison (trust accounts to file ledgers)
- Maintain list of clients with funds in trust account
- Retain for at least 6 years



9

Why?

Property Entrusted to Attorney

- Property of clients or third persons must be held in trust
 - R. Reg. Fla. Bar 5-1.1(a)(1)
- Prompt delivery to client or third person entitled to receipt
 - R. Reg. Fla. Bar 5-1.1(e)



10

What & For How Long?

Title Transactions

- Sec. 627.7845, F.S. (7 years)
 - Evidence of search; insurability; premium charged
- Agency agreement (10 years)
 - Issued products and supporting documents
 - Records, books of account, files, correspondence, and bank records



11

What & For How Long?

Title Transactions

- RESPA (lenders)
 - HUD-1 and related documents (5 years)
 - 12 C.F.R. Sec. 1024.10(e)
- TRID (lenders)
 - CD and related documents (5 years)
 - 12 C.F.R. Sec. 1026.25(c)(1)(ii)
- Lender closing instructions



12

What & For How Long?

Title Transactions

- FIRPTA (5 years*)
 - Certificate of non-foreign status
 - 26 C.F.R. Sec. 1.1445-2(b)(3)
- Form W-9 or substitute (4 years*)
 - For use with Form 1099-S
 - 26 C.F.R. Sec. 1.6045-4(l)(1)(iii)



* Commencing calendar year following year of closing



13

What	How Long?	Reference
Title transactions: evidence of search, insurability, premium	7 years	F.S. 627.7845
Title insurance products & supporting docs, records, correspondence, bank records, books of account	10 years	Old Republic Agency Agreement
Title transactions: HUD-1, Closing Disclosure, and related documents	5 years	12 C.F.R. Sec. 1024.10(e) and 12 C.F.R. Sec. 1026.25(c)(1)(ii)
IRS documents: FIRPTA forms - Certificate of Non-Foreign Status or Form 8288 for withholding	5 years (beginning the year after closing)	26 C.F.R. Sec. 1.1445-2(b)(3)
IRS documents: 1099-S and Form W-9 or substitute	4 years (beginning the year after closing)	26 C.F.R. Sec. 1.6045-4(l)(1)(iii)
Trust Accounts: reconciliations, comparisons, lists of clients with funds in trust account	6 years	R. Reg. Fla. Bar 5-1.2(d)

How? (Practical)

File management



- Assembling the file
- Closing activity
- Post closing activity
- Archiving the file
- Destroying archived file

How?

Assembling the file



- Open file upon receipt of contract or title request from lender.
- Title search documents and examination results
- Send file retention policy and obtain client consent
- Cull the file – don't keep what you don't need



16

How?

Closing Activity

- Copy and return identity and other personal documents
- Collect IRS documentation
 - FIRPTA
 - Form 1099-S
- Copy original executed documents



17

How?

Post Closing Activity

- Copy and forward recorded documents
- Check for recorded mortgage satisfaction(s)
- Client ledger balance to zero
 - Save ledger to file



18

How? Emails & Texts



Saving Email and text messages

- Same rules as paper
- Save emails as PDF for the digital file
- Backup text messages to your computer
- Save screen shots of important text messages



19

Text Messages

- Increasingly popular
- Why? Easy, Efficient, Effective
- Concerns – ethical obligations, confidentiality, record preservation
 - SMS/MMS messages are not secured
 - Need End-to-End Encryption – iMessage, WhatsApp, Signal



20

How?

Culling the file

- Remove and destroy unnecessary material
 - Copies of published material
 - Draft versions of final documents
 - Informal notes and other purely extraneous materials

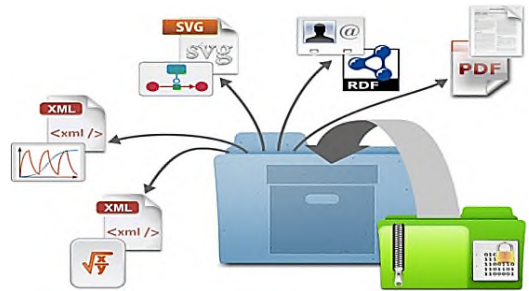


21

How?

Archiving the file

- Retain
 - Essential records of transaction
 - Zero balance ledger
 - File Closing Checklist
 - Calendar for future disposal
 - Convert to digital file - R.
- Regulating Fla. Bar 5-1.2(b)



22

Digital Copies

- Best Evidence Rule
 - Digital copies of original documents are allowed
 - Some documents like a Will or a Promissory Note must still be original
- Regular course of business
 - Sec. 627.7845(2), F.S.



23

Sample File Closing Checklist

- Confirm file ledger zero
- Confirm all docs sent to proper party (Deed, OP)
- Attorney Final Review
- Calendar intended destruction date

SAMPLE FILE CLOSING CHECKLIST		
Insured: _____	File #: _____	
Closer: _____	Date: _____	
ACTION	INITIALS	DATE
1. Change master file register from active to closed status and enter date and closed file number in closed file register.		
2. Confirm file ledger card reflects zero balance.		
3. Confirm all original documents filed or recorded.		
4. Confirm all third party property delivered (e.g. deeds, mortgages, policies, closing packages).		
5. Copy commitment, policies and examiner notes and file.		
6. Review file for documents to be included in forms system.		
7. Duplicate documents, unused note pads, etc., removed from file (DO NOT remove draft work product, memos, phone messages, research notes, etc.).		
8. Check for loose, unfilled documents and place in the file.		
9. If an unsatisfied judgment is involved, diary the file for 3, 6, and 9 years to review assets and renewal of judgment prior to the expiration of 10 years.		
10. If UCC is involved, diary the file for renewal of UCC filing.		
11. If the file involves a lease or option to buy, diary the file for 6 months prior to expiration.		
12. If the file involves a criminal matter, check to see if expungement is possible and diary the file for 3 years.		
13. Final review by lawyer for any further work to be done and closing letter to client with return of any original documents.		
14. Assign destruction date and enter into calendar system and/or mark in closed file register or on index card.		



24

Who owns the file?

- Original documents
- Supporting documents
- Office-created documents
- *Dowda and Fields v. Cobb*, 452 So.2d 1140 (Fla. 5th DCA 1984)
 - No obligation to surrender entire file to client.
 - “Client File” is the property of the law office.



25

File Destruction



- Client's wishes are paramount
- Client notification and authority to dispose should be obtained if possible
- FL Bar Ethics Opinions 81-8, 63-3 & 71-62



26

Practical: How?

- Destroying archived file
 - Review File Closing Checklist
 - Destroy in compliance with Safeguards Rule
 - Maintain evidence of file destruction
- What about digital files?



27

Digital Media Destruction

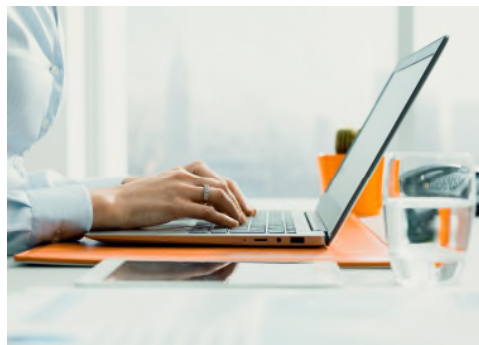


28

Destruction of Storage Media

- Devices must be sanitized

- Hard drives
- Copy machines
- Printers
- Scanners
- Cell Phones
- USB "thumb" drives



FL Bar Ethics Opinion 10-2



The Fund

29

What is Sanitization?



The National Institute of Standards and Technology (NIST) defines sanitization as: “the general process of removing data from storage media, such that there is reasonable assurance that the data may not be easily retrieved and reconstructed.”



30

Categories of Media Sanitization

	NIST 800-88 Description
Clearing	Clearing information is a level of media sanitization that would protect the confidentiality of information against a robust keyboard attack. Simple deletion of items would not suffice for clearing. For example, overwriting is an acceptable method for clearing media.
Purging	Purging information is a media sanitization process that protects the confidentiality of information against a laboratory attack. For some media, clearing media would not suffice for purging. Executing the firmware Secure Erase command (for ATA drives only) and degaussing are examples of acceptable methods for purging.
Destroying	Destruction of media is the ultimate form of sanitization. After media are destroyed, they cannot be reused as originally intended. Physical destruction can be accomplished using a variety of methods, including disintegration, incineration, pulverizing, shredding and melting.



31

What Next? Written Policies

- Information security program

- Ensure security & confidentiality
- Protect against threats & hazards
- Protect against unauthorized access



32

What Next? Written Policies

Information security program Requirements

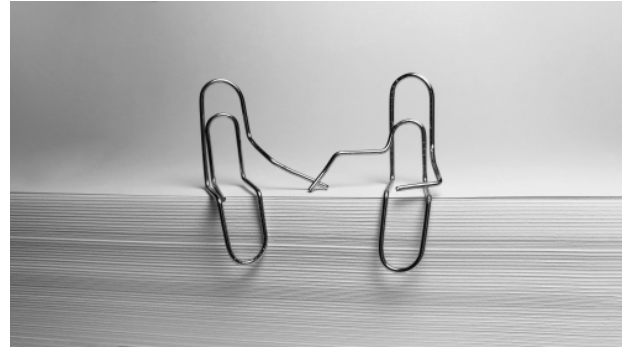
- Designate qualified coordinator
- Identify risks
- Design/implement safeguards
- Oversee service providers
- Evaluate after regular testing & adjust as needed



33

Put it in writing

- Privacy and Information Security Policy
- File Retention and Destruction Policy
- Client Acknowledgement and Consent to Destruction
- Notice of Archiving & Destruction
- Electronic File Policy



34

Sample Privacy and Information Security Policy

- Purpose
- Scope
- Procedures for Physical Security, Network Security and Disposal of NPI

Insert Business Entity Logo/Name Here

Policies and Procedures	
Privacy and Information Security	
Purpose	Document a privacy and information security program (policies and procedures) to help ensure (insert name of entity/agency) maintains written protocols for the protection of data and Non-public Personal Information (NPI).
Scope	These policies and procedures are for all of (insert name of entity/agency) (hereafter referred to as "The Company") locations including all satellite offices. These procedures are to be followed by all employees and independent contractors where applicable.
Procedures	<p>(The Company should review its legal, contractual, and statutory requirements for privacy and information security and incorporate those requirements in these procedures.)</p> <p>The Company has a formal privacy and information security program that is appropriate with the size and complexity, nature and scope of the Company's activities and the sensitivity of the information in the Company's possession. As part of this program, The Company maintains a Privacy Policy Notice (see a Notice) that is posted on The Company's website and provided to customers (see a Notice) for each order processed. Additional information about The Company's privacy and information security program is available to customers and customers upon request.</p> <p>The Company policies are approved with the privacy and information security program are given to all employees and the employees must acknowledge in writing that they have read and understand such policies. It is the responsibility of (insert role/function) to help ensure The Company has received all employee acknowledgements.</p> <p>The Company makes an assessment (insert frequency) of the standards and requirements utilized with The Company's information security program, including those set out in this policy and procedure document. This assessment is conducted by (insert role/function/vendor) and a formal report on compliance is issued to The Company management.</p> <p>Physical Security of NPI</p> <p>The Company utilizes (insert vendor name) as the information provider for background and credit checks. The Company individuals who have access to NPI is restricted to authorized personnel and employees who have undergone a formal background check and credit report process which identified no impediments.</p> <p>Removable media devices, including but not limited to external hard drives, compact discs, magnetic tapes and USB/flesh drives are issued by the Company with the approval of (insert role/function). The use of removable</p>

Home of This Company
Address or Website of This Company

82



35

Sample File Retention & Destruction Policy

- Policy statement
- Guidelines for Destruction
- Guidelines for Culling files
- Implementation of Policy

SAMPLE FILE RETENTION AND DESTRUCTION POLICY

Effective _____, this company implemented this file retention and destruction policy:

File Retention and Destruction Policy

Original documents and other property belonging to others are delivered or returned no later than the conclusion of the matter for which this company has been engaged. Copies of relevant materials which we create or receive will also be provided within that time frame. Our file on a matter is held in storage for a specific retention period. Prior to storage files are culled according to the Guidelines for Culling Files. At the end of the prescribed retention periods, files are summarily destroyed.

Guidelines for Destruction of Inactive Title Insurance Transaction Files

Purpose: Inactive title insurance transaction files may not be destroyed until the periods of time related to statutory, regulatory, contractual, and customer service guidelines have expired. This period of time ("retention period") commences on the date our work on a matter has been completed.

Procedure:

1. Files are archived until a regularly scheduled file destruction event arrives which is after a file's targeted destruction date.
2. The targeted destruction date is that date entered into the respective File Closing Checklist form or the date ten (10) years from the date of the conclusion of the matter, whichever period is longer, provided the respective File Closing Checklist indicates that the file has been sufficiently culled and is ready for destruction. The targeted destruction date will also have been entered upon the appropriate office calendars.
3. If the File Closing Checklist does not then indicate readiness, the file will be set aside and culled pursuant to the Guidelines for Culling Files and a new destruction date will be assigned.

Guidelines for Culling Files

Purpose: A stripped-down file contains only those materials needed for legitimate business purposes including statutory, regulatory, contractual, and customer service requirements. A culled file is ready for destruction at the end of its designated retention period with only a cursory review of its status as an appropriately culled file. As such, it may not then contain any property belonging to others.



36

Sample Acknowledgement & Consent

- Client acknowledgement of policy and consent
 - Statement of Policy
 - Document delivery
 - Post file closure
 - Limited storage time
 - Consent to Destruction

Acknowledgement of File Retention and Destruction Policy and Consent to File Destruction

In keeping with our commitment to keeping you informed, we are asking you to understand and acknowledge our responsibility as it relates to the continued maintenance of your file once this matter has concluded.

Please read the statement of policy below and sign where indicated to indicate your understanding of our file retention and destruction policy and your consent to its use as it relates to your transaction file.

POLICY

Original documents and other property belonging to you will be delivered to you no later than the conclusion of our work on this transaction at which time we will consider our file to be closed. Copies of relevant materials which we create, receive or are otherwise obligated to deliver will be provided to you within that time frame as well.

Any copy requests made by you after our file has been closed will be subject to the file's availability and our charge for retrieving and copying the requested materials. Our files are kept for the specific retention period we assign to each based upon regulatory compliance and other factors. At the end of assigned retention periods, files are destroyed.

PLEASE FEEL FREE TO ASK QUESTIONS BEFORE SIGNING THIS FORM.

I HEREBY ACKNOWLEDGE that I have read and understand the file retention and destruction policy adopted by this business and I CONSENT to the destruction of my transaction file in accordance with the policy.

(Name)

(Date)



37

Sample Archive & Destruction Notice

- Matter is concluded
- File moving to storage
- Offer to copy file and cost
- File subject to retention and destruction policy

CLOSED FILE ARCHIVE AND DESTRUCTION NOTICE

[Date]

[Addressee information]

Re:

Dear:

Our records indicate the above matter is concluded and I want to again thank you for the opportunity to have provided our services to you. I am writing to inform you that we are now in the process of moving the closed case file into archival storage. The file may include copies of records you want or need, such as documents we created for you. Please let us know within thirty (30) days of this letter's date whether you would like to obtain a copy of this file. The cost of copying will be billed to you at [xx] cents per page.

At the completion of the 30-day period, the file will be moved into off-site archival storage, and will then be subject to destruction according to the firm's record retention and destruction policy without further notice to you.

Thank you for your confidence in us.

Sincerely,



38

Sample Electronic File Policy

- Electronic file policy
 - Effective date
 - Policy statement
 - Paper document handling
 - Scanning process
 - File backups

Sample Electronic File Policy

[Company]

Effective: [Date]

Last revised: [Date]

1. Electronic Files

All files that we create and maintain relating to client, customer or consumer matters, as well as this office's internal procedures, financial matters, and operations guides, are stored electronically. An electronic file is this company's actual office file related to that matter.

All incoming and outgoing paper documents are scanned daily and added to the respective electronic files. After scanning, paper documents are placed into a matter's paper file folder. Document Originals are handled as described below.

The paper file folders and their contents are shredded from time to time in accordance with this company's File Retention Policy.

2. Scanning

After review, all paper documents are placed into the secure sorting box designated for scanning. By the end of each day, the paper documents will have been scanned and uploaded to the office server into an electronic file designated as the general file relating to that matter. Once a paper document is scanned and uploaded to the office server, the electronic document shall become part of the actual office file. The paper file, and the papers it contains, is merely for convenience until the matter's final resolution.

3. File Backups

All electronic files are backed up daily by synchronizing the entire server to an external hard drive, which is then taken offsite. There are seven external hard drives that are backed up in rotation and kept offsite as follows:

- Daily A and Daily B [specify offsite location]
- Weekly A and Weekly B [specify offsite location]
- Monthly A and Monthly B [specify offsite location]
- Annual [specify offsite location]



39

Fund Resources

Information Center

Search the Information Center

What's New

Digital Closings
Real estate closings are moving in the direction of less paper and more technology. Learn about digital closings and how to get your practice ready.

ALTA 2021 Forms
The Florida Office of Insurance Regulation (OIR) has approved the 2021 American Land Title Association (ALTA) forms for use in Florida. Stay up-to-date with the latest information.

Latest Updates
RON Notarial Certificates (.docx)
FAQ, RON and 2020 changes to Notarial...
ALTA Notarization Types and Terminology
RON Frequently Asked Questions

Latest News
ALTA Forms & Closing Software Chart
The What's Over The New 2021 ALTA...
2021 ALTA Forms & New Requirements
New ALTA 2021 Commitment Policies...

[Learn More](#)

Policies and Procedures	
Privacy and Information Security	
Purpose	Document a privacy and information security program (policies and procedures) to help ensure (insert name of entity/agency) maintains written protocols for the protection of data and Non-public Personal Information (NPI).
Scope	These policies and procedures are for all of (insert name of entity/agency) (hereafter referred to as "The Firm") locations including all satellite offices. These procedures are to be followed by all employees and independent contractors where applicable.
Procedures	<p><i>[The Firm should review its legal, contractual, and statutory requirements for privacy and information security and incorporate those requirements in these procedures.]</i></p> <p>The Firm has a formal privacy and information security program that is appropriate with the size and complexity, the nature and scope of The Firm's activities and the sensitivity of the information in The Firm's possession. As part of this program, The Firm maintains a Privacy Policy Notice (see attached) that is posted on The Firm's website and provided to customers and consumers for each order processed. Additional information about The Firm's privacy and information security program is available to consumers and customers upon request.</p> <p>The Firm's policies associated with the privacy and information security program are given to all employees and the employees must acknowledge in writing that they have read and understand such policies. It is the responsibility of (insert role/function) to help ensure The Firm has received all employee acknowledgements.</p> <p>The Firm makes an assessment (insert frequency) of the standards and requirements affiliated with The Firm's information security program, including those set out in this policy and procedure document. This assessment is conducted by (insert role/function/vendor) and a formal report on compliance is issued to The Firm management.</p> <p>Physical Security of NPI</p> <p>The Firm utilizes (insert vendor name) as the information provider for background and credit checks. The Firm individuals who have access to NPI are restricted to authorized principals and employees who have</p>



40

The Fund Real Estate Forum

A FREE Attorney-Members-Only email forum to exchange insights and information.

[Get Started!](#)

Join the Conversation

Interested in seeing the kinds of issues Fund Members across the state are dealing with...or have a question to pose to a group of Fund Members? **The Fund's Real Estate Forum is for you!** It is an incredible resource and it is FREE to join.

- 1. Sign up.** You must be an active Fund Member attorney.
- 2. Post a question.** Communicate and collaborate about Florida real estate law and practice.
- 3. Dialogue.** Exchange insights and information with Fund Member attorneys on legal matters affecting real estate transactions, litigation, and more.

That's all there is to it.


[Get Started!](#)

Focused on Florida's Real Estate Industry

- Sign up for the Real Estate Forum
- Post Questions and Answers



41


[Home](#)
[Info Center](#)
[Software](#)
[Services](#)
[Education](#)
[Resources](#)
[Support](#)
[Contact Us](#)
My Account (KScott@thefund.co)

The Fund Real Estate Forum

Forms Library

[Resources](#) > [Real Estate Forum](#) > Forms Library


Search for: [Search](#)

Form	
Affidavit Acknowledgment Format Category(s): Affidavits	Download
Affidavit of No Florida Estate Tax Due Category(s): Affidavits	Download
Affidavit of No Liens - DIL Category(s): Affidavits, "Deed-in-Lieu Package"	Download
Affidavit Regarding Credit Line Advances Category(s): Affidavits, Financing	Download
Agreement to Vacate the Premises - DIL Category(s): Affidavits, "Deed-in-Lieu Package"	Download
Arm's Length Affidavit Category(s): Affidavits	Download
Assignment and Assumption of Leases and Security Deposits Category(s): "Commercial Forms", Leases	Download
Assignment of Contract - Alternate Version Category(s): Agreements	Download

Filter by Category

- ☐ Affidavits
- ☐ Agreements
- ☐ Best Practices
- ☐ Commercial Forms
- ☐ Construction
- ☐ Conveyances
- ☐ Deed-in-Lieu Package
- ☐ Financing
- ☐ Leases
- ☐ Liens Claims
- ☐ Miscellaneous
- ☐ Mobile Homes
- ☐ Power of Attorney
- ☐ Trusts

- Forms Library
- Download Forms in Microsoft Word format



42

Thank you!

KScott@TheFund.com

(407) 240-3863 Ext. 7180



43

R. Regul. FL. Bar 4-1.6

As amended through July 6, 2023

Rule 4-1.6 - CONFIDENTIALITY OF INFORMATION(a)Consent Required to Reveal

Information. A lawyer must not reveal information relating to a client's representation except as stated in subdivisions (b), (c), and (d), unless the client gives informed consent.(b)When

Lawyer Must Reveal Information. A lawyer must reveal confidential information to the extent the lawyer reasonably believes necessary to:(1) prevent a client from committing a crime; or(2) prevent a death or substantial bodily harm.(c)When Lawyer May Reveal Information. A lawyer may reveal confidential information to the extent the lawyer reasonably believes necessary to:(1) serve the client's interest unless it is information the client specifically requires not to be disclosed;(2) establish a claim or defense on the lawyer's behalf in a controversy between the lawyer and client;(3) establish a defense to a criminal charge or civil claim against the lawyer based on conduct in which the client was involved;(4) respond to allegations in any proceeding concerning the lawyer's representation of the client;(5) comply with the Rules Regulating The Florida Bar;(6) detect and resolve conflicts of interest between lawyers in different firms arising from the lawyer's change of employment or from changes in the composition or ownership of a firm, but only if the revealed information would not compromise the attorneyclient privilege or otherwise prejudice the client; or(7) respond to specific allegations published via the internet by a former client (e.g. a negative online review) that the lawyer has engaged in criminal conduct punishable by law.(d)Exhaustion of Appellate Remedies. When required by a tribunal to reveal confidential information, a lawyer may first exhaust all appellate remedies.(e)Inadvertent Disclosure of Information. A lawyer must make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the client's representation.(f)Limitation on Amount of Disclosure. When disclosure is mandated or permitted, the lawyer must disclose no more information than is required to meet the requirements or accomplish the purposes of this rule.

R. Regul. FL. Bar 4-1.6

Amended July 23, 1992, effective 1/1/1993 (605 So.2d 252); amended Oct. 20, 1994 (644 So.2d 282); March 23, 2006, effective 5/22/2006 (933 So.2d 417); amended July 7, 2011, effective 10/1/2011 (67 So. 3d 1037); amended May 29, 2014, effective 6/1/2014 (140 So. 3d 541); amended June 11, 2015, effective 10/1/2015 (167 So.3d 412); amended March 16, 2023, effective 5/15/2023 (SC22-1292).

Comment

The lawyer is part of a judicial system charged with upholding the law. One of the lawyer's functions is to advise clients so that they avoid any violation of the law in the proper exercise of their rights.

This rule governs the disclosure by a lawyer of information relating to the representation of a client during the lawyer's representation of the client. See rule 4-1.18 for the lawyer's duties with respect to information provided to the lawyer by a prospective client, rule 4-1.9(c) for the lawyer's duty not to reveal information relating to the lawyer's prior representation of a former

client, and rules 4-1.8(b) and 4-1.9(b) for the lawyer's duties with respect to the use of confidential information to the disadvantage of clients and former clients.

A fundamental principle in the client-lawyer relationship is that, in the absence of the client's informed consent, the lawyer must not reveal information relating to the representation. See terminology for the definition of informed consent. This contributes to the trust that is the hallmark of the client-lawyer relationship. The client is thereby encouraged to seek legal assistance and to communicate fully and frankly with the lawyer even as to embarrassing or legally damaging subject matter. The lawyer needs this information to represent the client effectively and, if necessary, to advise the client to refrain from wrongful conduct. Almost without exception, clients come to lawyers in order to determine their rights and what is, in the complex of laws and regulations, deemed to be legal and correct. Based on experience, lawyers know that almost all clients follow the advice given, and the law is upheld.

The principle of confidentiality is given effect in 2 related bodies of law, the attorney-client privilege (which includes the work product doctrine) in the law of evidence and the rule of confidentiality established in professional ethics. The attorney-client privilege applies in judicial and other proceedings in which a lawyer may be called as a witness or otherwise required to produce evidence concerning a client. The rule of client-lawyer confidentiality applies in situations other than those where evidence is sought from the lawyer through compulsion of law. The confidentiality rule applies not merely to matters communicated in confidence by the client but also to all information relating to the representation, whatever its source. A lawyer may not disclose confidential information except as authorized or required by the Rules Regulating The Florida Bar or by law. However, none of the foregoing limits the requirement of disclosure in subdivision (b). This disclosure is required to prevent a lawyer from becoming an unwitting accomplice in the fraudulent acts of a client. See also Scope.

The requirement of maintaining confidentiality of information relating to representation applies to government lawyers who may disagree with the policy goals that their representation is designed to advance.

Authorized disclosure

A lawyer is impliedly authorized to make disclosures about a client when appropriate in carrying out the representation, except to the extent that the client's instructions or special circumstances limit that authority. In litigation, for example, a lawyer may disclose information by admitting a fact that cannot properly be disputed or in negotiation by making a disclosure that facilitates a satisfactory conclusion.

Lawyers in a firm may, in the course of the firm's practice, disclose to each other information relating to a client of the firm, unless the client has instructed that particular information be confined to specified lawyers.

Disclosure adverse to client

The confidentiality rule is subject to limited exceptions. In becoming privy to information about a client, a lawyer may foresee that the client intends serious harm to another person. However, to the extent a lawyer is required or permitted to disclose a client's purposes, the client will be inhibited from revealing facts that would enable the lawyer to counsel against a wrongful course of action. While the public may be protected if full and open communication by the client is encouraged, several situations must be distinguished.

First, the lawyer may not counsel or assist a client in conduct that is criminal or fraudulent. See rule 4-1.2(d). Similarly, a lawyer has a duty under rule 4-3.3(a)(4) not to use false evidence. This duty is essentially a special instance of the duty prescribed in rule 4-1.2(d) to avoid assisting a client in criminal or fraudulent conduct.

Second, the lawyer may have been innocently involved in past conduct by the client that was criminal or fraudulent. In this situation the lawyer has not violated rule 4-1.2(d), because to "counsel or assist" criminal or fraudulent conduct requires knowing that the conduct is of that character.

Third, the lawyer may learn that a client intends prospective conduct that is criminal. As stated in subdivision (b)(1), the lawyer must reveal information in order to prevent these consequences. It is admittedly difficult for a lawyer to "know" when the criminal intent will actually be carried out, for the client may have a change of mind.

Subdivision (b)(2) contemplates past acts on the part of a client that may result in present or future consequences that may be avoided by disclosure of otherwise confidential communications. Rule 4-1.6(b)(2) would now require the lawyer to disclose information reasonably necessary to prevent the future death or substantial bodily harm to another, even though the act of the client has been completed.

The lawyer's exercise of discretion requires consideration of such factors as the nature of the lawyer's relationship with the client and with those who might be injured by the client, the lawyer's own involvement in the transaction, and factors that may extenuate the conduct in question. Where practical the lawyer should seek to persuade the client to take suitable action. In any case, a disclosure adverse to the client's interest should be no greater than the lawyer reasonably believes necessary to the purpose.

Withdrawal

If the lawyer's services will be used by the client in materially furthering a course of criminal or fraudulent conduct, the lawyer must withdraw, as stated in rule 4-1.16(a)(1).

After withdrawal the lawyer is required to refrain from making disclosure of the client's confidences, except as otherwise provided in rule 4-1.6. Neither this rule nor rule 4-1.8(b) nor rule 4-1.16(d) prevents the lawyer from giving notice of the fact of withdrawal, and the lawyer may also withdraw or disaffirm any opinion, document, affirmation, or the like.

Where the client is an organization, the lawyer may be in doubt whether contemplated conduct will actually be carried out by the organization. Where necessary to guide conduct in connection with the rule, the lawyer may make inquiry within the organization as indicated in rule 4-1.13(b).

Dispute concerning lawyer's conduct

A lawyer's confidentiality obligations do not preclude a lawyer from securing confidential legal advice about the lawyer's personal responsibility to comply with these rules. In most situations, disclosing information to secure this advice will be impliedly authorized for the lawyer to carry out the representation. Even when the disclosure is not impliedly authorized, subdivision (c)(5) permits this disclosure because of the importance of a lawyer's compliance with the Rules of Professional Conduct.

Where a legal claim or disciplinary charge alleges complicity of the lawyer in a client's conduct or other misconduct of the lawyer involving representation of the client, the lawyer may respond to the extent the lawyer reasonably believes necessary to establish a defense. The same is true

with respect to a claim involving the conduct or representation of a former client. The lawyer's right to respond arises when an assertion of complicity has been made. Subdivision (c) does not require the lawyer to await the commencement of an action or proceeding that charges complicity, so that the defense may be established by responding directly to a third party who has made the assertion. The right to defend, of course, applies where a proceeding has been commenced. Where practicable and not prejudicial to the lawyer's ability to establish the defense, the lawyer should advise the client of the third party's assertion and request that the client respond appropriately. In any event, disclosure should be no greater than the lawyer reasonably believes is necessary to vindicate innocence, the disclosure should be made in a manner that limits access to the information to the tribunal or other persons having a need to know it, and appropriate protective orders or other arrangements should be sought by the lawyer to the fullest extent practicable.

If the lawyer is charged with wrongdoing in which the client's conduct is implicated, the rule of confidentiality should not prevent the lawyer from defending against the charge. A charge can arise in a civil, criminal, or professional disciplinary proceeding and can be based on a wrong allegedly committed by the lawyer against the client or on a wrong alleged by a third person; for example, a person claiming to have been defrauded by the lawyer and client acting together. A lawyer entitled to a fee is permitted by subdivision (c) to prove the services rendered in an action to collect it. This aspect of the rule expresses the principle that the beneficiary of a fiduciary relationship may not exploit it to the detriment of the fiduciary. As stated above, the lawyer must make every effort practicable to avoid unnecessary disclosure of information relating to a representation, to limit disclosure to those having the need to know it, and to obtain protective orders or make other arrangements minimizing the risk of disclosure.

Subdivision (c)(7) allows a lawyer to respond to specific allegations published via the internet by a former client (e.g. a negative online review) that the lawyer has engaged in criminal conduct punishable by law. However, under subdivision (f), even when the lawyer is operating within the scope of the (c)(7) exception, disclosure must be no greater than the lawyer reasonably believes necessary to refute the specific allegations.

Disclosures otherwise required or authorized

The attorney-client privilege is differently defined in various jurisdictions. If a lawyer is called as a witness to give testimony concerning a client, absent waiver by the client, rule 4-1.6(a) requires the lawyer to invoke the privilege when it is applicable. The lawyer must comply with the final orders of a court or other tribunal of competent jurisdiction requiring the lawyer to give information about the client.

The Rules of Professional Conduct in various circumstances permit or require a lawyer to disclose information relating to the representation. See rules 4-2.3, 4-3.3, and 4-4.1. In addition to these provisions, a lawyer may be obligated or permitted by other provisions of law to give information about a client. Whether another provision of law supersedes rule 4-1.6 is a matter of interpretation beyond the scope of these rules, but a presumption should exist against a supersession.

Detection of Conflicts of Interest

Subdivision (c)(6) recognizes that lawyers in different firms may need to disclose limited information to each other to detect and resolve conflicts of interest, for example, when a lawyer

is considering an association with another firm, two or more firms are considering a merger, or a lawyer is considering the purchase of a law practice. See comment to rule 4-1.17. Under these circumstances, lawyers and law firms are permitted to disclose limited information, but only once substantive discussions regarding the new relationship have occurred. Any disclosure should ordinarily include no more than the identity of the persons and entities involved in a matter, a brief summary of the general issues involved, and information about whether the matter has terminated. Even this limited information, however, should be disclosed only to the extent reasonably necessary to detect and resolve conflicts of interest that might arise from the possible new relationship. The disclosure of any information is prohibited if it would compromise the attorney-client privilege or otherwise prejudice the client (e.g., the fact that a corporate client is seeking advice on a corporate takeover that has not been publicly announced; that a person has consulted a lawyer about the possibility of divorce before the person's intentions are known to the person's spouse; or that a person has consulted a lawyer about a criminal investigation that has not led to a public charge). Under those circumstances, subdivision (a) prohibits disclosure unless the client or former client gives informed consent. A lawyer's fiduciary duty to the lawyer's firm may also govern a lawyer's conduct when exploring an association with another firm and is beyond the scope of these rules.

Any information disclosed under this subdivision may be used or further disclosed only to the extent necessary to detect and resolve conflicts of interest. This subdivision does not restrict the use of information acquired by means independent of any disclosure under this subdivision. This subdivision also does not affect the disclosure of information within a law firm when the disclosure is otherwise authorized, for example, when a lawyer in a firm discloses information to another lawyer in the same firm to detect and resolve conflicts of interest that could arise in connection with undertaking a new representation.

Acting Competently to Preserve Confidentiality

Paragraph (e) requires a lawyer to act competently to safeguard information relating to the representation of a client against unauthorized access by third parties and against inadvertent or unauthorized disclosure by the lawyer or other persons who are participating in the representation of the client or who are subject to the lawyer's supervision. See rules 4-1.1, 4-5.1 and 4-5.3. The unauthorized access to, or the inadvertent or unauthorized disclosure of, information relating to the representation of a client does not constitute a violation of paragraph (e) if the lawyer has made reasonable efforts to prevent the access or disclosure. Factors to be considered in determining the reasonableness of the lawyer's efforts include, but are not limited to, the sensitivity of the information, the likelihood of disclosure if additional safeguards are not employed, the cost of employing additional safeguards, the difficulty of implementing the safeguards, and the extent to which the safeguards adversely affect the lawyer's ability to represent clients (e.g., by making a device or important piece of software excessively difficult to use). A client may require the lawyer to implement special security measures not required by this rule or may give informed consent to forgo security measures that would otherwise be required by this rule. Whether a lawyer may be required to take additional steps to safeguard a client's information in order to comply with other law, for example state and federal laws that govern data privacy or that impose notification requirements on the loss of, or unauthorized access to,

electronic information, is beyond the scope of these rules. For a lawyer's duties when sharing information with nonlawyers outside the lawyer's own firm, see the comment to rule 4-5.3. When transmitting a communication that includes information relating to the representation of a client, the lawyer must take reasonable precautions to prevent the information from coming into the hands of unintended recipients. This duty, however, does not require that the lawyer use special security measures if the method of communication affords a reasonable expectation of privacy. Special circumstances, however, may warrant special precautions. Factors to be considered in determining the reasonableness of the lawyer's expectation of confidentiality include the sensitivity of the information and the extent to which the privacy of the communication is protected by law or by a confidentiality agreement. A client may require the lawyer to implement special security measures not required by this rule or may give informed consent to the use of a means of communication that would otherwise be prohibited by this rule. Whether a lawyer may be required to take additional steps in order to comply with other law, for example state and federal laws that govern data privacy, is beyond the scope of these rules.

Former client

The duty of confidentiality continues after the client-lawyer relationship has terminated. See rule 4-1.9 for the prohibition against using such information to the disadvantage of the former client.

RT 314—STANDARDS FOR SAFEGUARDING CUSTOMER INFORMATION

Authority: 15 U.S.C. 6801(b), 6805(b)(2).

Source: 67 FR 36493, May 23, 2002, unless otherwise noted.

Enhanced Content - Content Tools

URL <https://www.ecfr.gov/current/title-16/section-314.1>

Citation 16 CFR 314.1

§ 314.1 Purpose and scope.

(a) Purpose. This part, which implements sections 501 and 505(b)(2) of the Gramm-Leach-Bliley Act, sets forth standards for developing, implementing, and maintaining reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of customer information.

(b) Scope. This part applies to the handling of customer information by all financial institutions over which the Federal Trade Commission (“FTC” or “Commission”) has jurisdiction. Namely, this part applies to those “financial institutions” over which the Commission has rulemaking authority pursuant to section 501(b) of the Gramm-Leach-Bliley Act. An entity is a “financial institution” if its business is engaging in an activity that is financial in nature or incidental to such financial activities as described in section 4(k) of the Bank Holding Company Act of 1956, 12 U.S.C. 1843(k), which incorporates activities enumerated by the Federal Reserve Board in 12 CFR 225.28 and 225.86. The “financial institutions” subject to the Commission’s enforcement authority are those that are not otherwise subject to the enforcement authority of another regulator under section 505 of the Gramm-Leach-Bliley Act, 15 U.S.C. 6805. More specifically, those entities include, but are not limited to, mortgage lenders, “pay day” lenders, finance companies, mortgage brokers, account servicers, check cashers, wire transferors, travel agencies operated in connection with financial services, collection agencies, credit counselors and other financial advisors, tax preparation firms, non-federally insured credit unions, investment advisors that are not required to register with the Securities and Exchange Commission, and entities acting as finders. They are referred to in this part as “You.” This part applies to all customer information in your possession, regardless of whether such information pertains to individuals with whom you have a customer relationship, or pertains to the customers of other financial institutions that have provided such information to you.

[67 FR 36493, May 23, 2002, as amended at 86 FR 70304, Dec. 9, 2021]

§ 314.2 Definitions.

(a) Authorized user means any employee, contractor, agent, customer, or other person that is authorized to access any of your information systems or data.

(b)

(1) Consumer means an individual who obtains or has obtained a financial product or service from you that is to be used primarily for personal, family, or household purposes, or that individual's legal representative.

(2) For example:

(i) An individual who applies to you for credit for personal, family, or household purposes is a consumer of a financial service, regardless of whether the credit is extended.

(ii) An individual who provides nonpublic personal information to you in order to obtain a determination about whether he or she may qualify for a loan to be used primarily for personal, family, or household purposes is a consumer of a financial service, regardless of whether the loan is extended.

(iii) An individual who provides nonpublic personal information to you in connection with obtaining or seeking to obtain financial, investment, or economic advisory services is a consumer, regardless of whether you establish a continuing advisory relationship.

(iv) If you hold ownership or servicing rights to an individual's loan that is used primarily for personal, family, or household purposes, the individual is your consumer, even if you hold those rights in conjunction with one or more other institutions. (The individual is also a consumer with respect to the other financial institutions involved.) An individual who has a loan in which you have ownership or servicing rights is your consumer, even if you, or another institution with those rights, hire an agent to collect on the loan.

(v) An individual who is a consumer of another financial institution is not your consumer solely because you act as agent for, or provide processing or other services to, that financial institution.

(vi) An individual is not your consumer solely because he or she has designated you as trustee for a trust.

(vii) An individual is not your consumer solely because he or she is a beneficiary of a trust for which you are a trustee.

(viii) An individual is not your consumer solely because he or she is a participant or a beneficiary of an employee benefit plan that you sponsor or for which you act as a trustee or fiduciary.

(c) Customer means a consumer who has a customer relationship with you.

(d) Customer information means any record containing nonpublic personal information about a customer of a financial institution, whether in paper, electronic, or other form, that is handled or maintained by or on behalf of you or your affiliates.

(e)

(1) Customer relationship means a continuing relationship between a consumer and you under which you provide one or more financial products or services to the consumer that are to be used primarily for personal, family, or household purposes.

(2) For example:

(i) Continuing relationship. A consumer has a continuing relationship with you if the consumer:

(A) Has a credit or investment account with you;

(B) Obtains a loan from you;

(C) Purchases an insurance product from you;

(D) Holds an investment product through you, such as when you act as a custodian for securities or for assets in an Individual Retirement Arrangement;

(E) Enters into an agreement or understanding with you whereby you undertake to arrange or broker a home mortgage loan, or credit to purchase a vehicle, for the consumer;

(F) Enters into a lease of personal property on a non-operating basis with you;

(G) Obtains financial, investment, or economic advisory services from you for a fee;

(H) Becomes your client for the purpose of obtaining tax preparation or credit counseling services from you;

(I) Obtains career counseling while seeking employment with a financial institution or the finance, accounting, or audit department of any company (or while employed by such a financial institution or department of any company);

(J) Is obligated on an account that you purchase from another financial institution, regardless of whether the account is in default when purchased, unless you do not locate the consumer or attempt to collect any amount from the consumer on the account;

(K) Obtains real estate settlement services from you; or

(L) Has a loan for which you own the servicing rights.

(ii) No continuing relationship. A consumer does not, however, have a continuing relationship with you if:

(A) The consumer obtains a financial product or service from you only in isolated transactions, such as using your ATM to withdraw cash from an account at another financial institution; purchasing a money order from you; cashing a check with you; or making a wire transfer through you;

(B) You sell the consumer's loan and do not retain the rights to service that loan;

(C) You sell the consumer airline tickets, travel insurance, or traveler's checks in isolated transactions;

(D) The consumer obtains one-time personal or real property appraisal services from you; or

(E) The consumer purchases checks for a personal checking account from you.

(f) Encryption means the transformation of data into a form that results in a low probability of assigning meaning without the use of a protective process or key, consistent with current cryptographic standards and accompanied by appropriate safeguards for cryptographic key material.

(g)

(1) Financial product or service means any product or service that a financial holding company could offer by engaging in a financial activity under section 4(k) of the Bank Holding Company Act of 1956 (12 U.S.C. 1843(k)).

(2) Financial service includes your evaluation or brokerage of information that you collect in connection with a request or an application from a consumer for a financial product or service.

(h)

(1) Financial institution means any institution the business of which is engaging in an activity that is financial in nature or incidental to such financial activities as described in section 4(k) of the Bank Holding Company Act of 1956, 12 U.S.C. 1843(k). An institution that is significantly engaged in financial activities, or significantly engaged in activities incidental to such financial activities, is a financial institution.

(2) Examples of financial institutions are as follows:

(i) A retailer that extends credit by issuing its own credit card directly to consumers is a financial institution because extending credit is a financial activity listed in 12 CFR 225.28(b)(1) and referenced in section 4(k)(4)(F) of the Bank Holding Company Act of 1956 (12 U.S.C. 1843(k)(4)(F)), and issuing that extension of credit through a proprietary credit card demonstrates that a retailer is significantly engaged in extending credit.

(ii) An automobile dealership that, as a usual part of its business, leases automobiles on a nonoperating basis for longer than 90 days is a financial institution with respect to its leasing business because leasing personal property on a nonoperating basis where the initial term of the lease is at least 90 days is a financial activity listed in 12 CFR 225.28(b)(3) and referenced in section 4(k)(4)(F) of the Bank Holding Company Act, 12 U.S.C. 1843(k)(4)(F).

(iii) A personal property or real estate appraiser is a financial institution because real and personal property appraisal is a financial activity listed in 12 CFR 225.28(b)(2)(i) and referenced in section 4(k)(4)(F) of the Bank Holding Company Act, 12 U.S.C. 1843(k)(4)(F).

(iv) A career counselor that specializes in providing career counseling services to individuals currently employed by or recently displaced from a financial organization, individuals who are seeking employment with a financial organization, or individuals who are currently employed by or seeking placement with the finance, accounting or audit departments of any company is a financial institution because such career counseling activities are financial activities listed in 12 CFR 225.28(b)(9)(iii) and referenced in section 4(k)(4)(F) of the Bank Holding Company Act, 12 U.S.C. 1843(k)(4)(F).

(v) A business that prints and sells checks for consumers, either as its sole business or as one of its product lines, is a financial institution because printing and selling checks is a financial activity that is listed in 12 CFR 225.28(b)(10)(ii) and referenced in section 4(k)(4)(F) of the Bank Holding Company Act, 12 U.S.C. 1843(k)(4)(F).

(vi) A business that regularly wires money to and from consumers is a financial institution because transferring money is a financial activity referenced in section 4(k)(4)(A) of the Bank Holding Company Act, 12 U.S.C. 1843(k)(4)(A), and regularly providing that service demonstrates that the business is significantly engaged in that activity.

(vii) A check cashing business is a financial institution because cashing a check is exchanging money, which is a financial activity listed in section 4(k)(4)(A) of the Bank Holding Company Act, 12 U.S.C. 1843(k)(4)(A).

(viii) An accountant or other tax preparation service that is in the business of completing income tax returns is a financial institution because tax preparation services is a financial activity listed

in 12 CFR 225.28(b)(6)(vi) and referenced in section 4(k)(4)(G) of the Bank Holding Company Act, 12 U.S.C. 1843(k)(4)(G).

(ix) A business that operates a travel agency in connection with financial services is a financial institution because operating a travel agency in connection with financial services is a financial activity listed in 12 CFR 225.86(b)(2) and referenced in section 4(k)(4)(G) of the Bank Holding Company Act, 12 U.S.C. 1843(k)(4)(G).

(x) An entity that provides real estate settlement services is a financial institution because providing real estate settlement services is a financial activity listed in 12 CFR 225.28(b)(2)(viii) and referenced in section 4(k)(4)(F) of the Bank Holding Company Act, 12 U.S.C. 1843(k)(4)(F).

(xi) A mortgage broker is a financial institution because brokering loans is a financial activity listed in 12 CFR 225.28(b)(1) and referenced in section 4(k)(4)(F) of the Bank Holding Company Act, 12 U.S.C. 1843(k)(4)(F).

(xii) An investment advisory company and a credit counseling service are each financial institutions because providing financial and investment advisory services are financial activities referenced in section 4(k)(4)(C) of the Bank Holding Company Act, 12 U.S.C. 1843(k)(4)(C).

(xiii) A company acting as a finder in bringing together one or more buyers and sellers of any product or service for transactions that the parties themselves negotiate and consummate is a financial institution because acting as a finder is an activity that is financial in nature or incidental to a financial activity listed in 12 CFR 225.86(d)(1).

(3) Financial institution does not include:

(i) Any person or entity with respect to any financial activity that is subject to the jurisdiction of the Commodity Futures Trading Commission under the Commodity Exchange Act (7 U.S.C. 1 et seq.);

(ii) The Federal Agricultural Mortgage Corporation or any entity chartered and operating under the Farm Credit Act of 1971 (12 U.S.C. 2001 et seq.);

(iii) Institutions chartered by Congress specifically to engage in securitizations, secondary market sales (including sales of servicing rights) or similar transactions related to a transaction of a consumer, as long as such institutions do not sell or transfer nonpublic personal information to a nonaffiliated third party other than as permitted by §§ 313.14 and 313.15; or

(iv) Entities that engage in financial activities but that are not significantly engaged in those financial activities, and entities that engage in activities incidental to financial activities but that are not significantly engaged in activities incidental to financial activities.

(4) Examples of entities that are not significantly engaged in financial activities are as follows:

(i) A retailer is not a financial institution if its only means of extending credit are occasional “lay away” and deferred payment plans or accepting payment by means of credit cards issued by others.

(ii) A retailer is not a financial institution merely because it accepts payment in the form of cash, checks, or credit cards that it did not issue.

(iii) A merchant is not a financial institution merely because it allows an individual to “run a tab.”

(iv) A grocery store is not a financial institution merely because it allows individuals to whom it sells groceries to cash a check, or write a check for a higher amount than the grocery purchase and obtain cash in return.

(i) Information security program means the administrative, technical, or physical safeguards you use to access, collect, distribute, process, protect, store, use, transmit, dispose of, or otherwise handle customer information.

(j) Information system means a discrete set of electronic information resources organized for the collection, processing, maintenance, use, sharing, dissemination or disposition of electronic information containing customer information or connected to a system containing customer information, as well as any specialized system such as industrial/process controls systems, telephone switching and private branch exchange systems, and environmental controls systems that contains customer information or that is connected to a system that contains customer information.

(k) Multi-factor authentication means authentication through verification of at least two of the following types of authentication factors:

(1) Knowledge factors, such as a password;

(2) Possession factors, such as a token; or

(3) Inherence factors, such as biometric characteristics.

(l)

(1) Nonpublic personal information means:

(i) Personally identifiable financial information; and

(ii) Any list, description, or other grouping of consumers (and publicly available information pertaining to them) that is derived using any personally identifiable financial information that is not publicly available.

(2) Nonpublic personal information does not include:

(i) Publicly available information, except as included on a list described in paragraph (l)(1)(ii) of this section; or

(ii) Any list, description, or other grouping of consumers (and publicly available information pertaining to them) that is derived without using any personally identifiable financial information that is not publicly available.

(3) For example:

(i) Nonpublic personal information includes any list of individuals' names and street addresses that is derived in whole or in part using personally identifiable financial information (that is not publicly available), such as account numbers.

(ii) Nonpublic personal information does not include any list of individuals' names and addresses that contains only publicly available information, is not derived, in whole or in part, using personally identifiable financial information that is not publicly available, and is not disclosed in a manner that indicates that any of the individuals on the list is a consumer of a financial institution.

(m) Penetration testing means a test methodology in which assessors attempt to circumvent or defeat the security features of an information system by attempting penetration of databases or controls from outside or inside your information systems.

(n)

(1) Personally identifiable financial information means any information:

(i) A consumer provides to you to obtain a financial product or service from you;

(ii) About a consumer resulting from any transaction involving a financial product or service between you and a consumer; or

(iii) You otherwise obtain about a consumer in connection with providing a financial product or service to that consumer.

(2) For example:

(i) Information included. Personally identifiable financial information includes:

(A) Information a consumer provides to you on an application to obtain a loan, credit card, or other financial product or service;

(B) Account balance information, payment history, overdraft history, and credit or debit card purchase information;

(C) The fact that an individual is or has been one of your customers or has obtained a financial product or service from you;

(D) Any information about your consumer if it is disclosed in a manner that indicates that the individual is or has been your consumer;

(E) Any information that a consumer provides to you or that you or your agent otherwise obtain in connection with collecting on, or servicing, a credit account;

(F) Any information you collect through an internet “cookie” (an information collecting device from a web server); and

(G) Information from a consumer report.

(ii) Information not included. Personally identifiable financial information does not include:

(A) A list of names and addresses of customers of an entity that is not a financial institution; and

(B) Information that does not identify a consumer, such as aggregate information or blind data that does not contain personal identifiers such as account numbers, names, or addresses.

(o)

(1) Publicly available information means any information that you have a reasonable basis to believe is lawfully made available to the general public from:

(i) Federal, State, or local government records;

(ii) Widely distributed media; or

(iii) Disclosures to the general public that are required to be made by Federal, State, or local law.

(2) You have a reasonable basis to believe that information is lawfully made available to the general public if you have taken steps to determine:

(i) That the information is of the type that is available to the general public; and

(ii) Whether an individual can direct that the information not be made available to the general public and, if so, that your consumer has not done so.

(3) For example:

(i) Government records. Publicly available information in government records includes information in government real estate records and security interest filings.

(ii) Widely distributed media. Publicly available information from widely distributed media includes information from a telephone book, a television or radio program, a newspaper, or a website that is available to the general public on an unrestricted basis. A website is not restricted merely because an internet service provider or a site operator requires a fee or a password, so long as access is available to the general public.

(iii) Reasonable basis.

(A) You have a reasonable basis to believe that mortgage information is lawfully made available to the general public if you have determined that the information is of the type included on the public record in the jurisdiction where the mortgage would be recorded.

(B) You have a reasonable basis to believe that an individual's telephone number is lawfully made available to the general public if you have located the telephone number in the telephone book or the consumer has informed you that the telephone number is not unlisted.

(p) Security event means an event resulting in unauthorized access to, or disruption or misuse of, an information system, information stored on such information system, or customer information held in physical form.

(q) Service provider means any person or entity that receives, maintains, processes, or otherwise is permitted access to customer information through its provision of services directly to a financial institution that is subject to this part.

(r) You includes each “financial institution” (but excludes any “other person”) over which the Commission has enforcement jurisdiction pursuant to section 505(a)(7) of the Gramm-Leach-Bliley Act.

[86 FR 70304, Dec. 9, 2021]

§ 314.3 Standards for safeguarding customer information.

(a) Information security program. You shall develop, implement, and maintain a comprehensive information security program that is written in one or more readily accessible parts and contains administrative, technical, and physical safeguards that are appropriate to your size and complexity, the nature and scope of your activities, and the sensitivity of any customer information at issue. The information security program shall include the elements set forth in § 314.4 and shall be reasonably designed to achieve the objectives of this part, as set forth in paragraph (b) of this section.

(b) Objectives. The objectives of section 501(b) of the Act, and of this part, are to:

- (1) Insure the security and confidentiality of customer information;
- (2) Protect against any anticipated threats or hazards to the security or integrity of such information; and
- (3) Protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer.

[67 FR 36493, May 23, 2002, as amended at 86 FR 70307, Dec. 9, 2021]

§ 314.4 Elements.

In order to develop, implement, and maintain your information security program, you shall:

(a) Designate a qualified individual responsible for overseeing and implementing your information security program and enforcing your information security program (for purposes of this part, “Qualified Individual”). The Qualified Individual may be employed by you, an affiliate, or a service provider. To the extent the requirement in this paragraph (a) is met using a service provider or an affiliate, you shall:

- (1) Retain responsibility for compliance with this part;
- (2) Designate a senior member of your personnel responsible for direction and oversight of the Qualified Individual; and
- (3) Require the service provider or affiliate to maintain an information security program that protects you in accordance with the requirements of this part.

(b) Base your information security program on a risk assessment that identifies reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that could result in the unauthorized disclosure, misuse, alteration, destruction, or other compromise of such information, and assesses the sufficiency of any safeguards in place to control these risks.

(1) The risk assessment shall be written and shall include:

(i) Criteria for the evaluation and categorization of identified security risks or threats you face;

(ii) Criteria for the assessment of the confidentiality, integrity, and availability of your information systems and customer information, including the adequacy of the existing controls in the context of the identified risks or threats you face; and

(iii) Requirements describing how identified risks will be mitigated or accepted based on the risk assessment and how the information security program will address the risks.

(2) You shall periodically perform additional risk assessments that reexamine the reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that could result in the unauthorized disclosure, misuse, alteration, destruction, or other compromise of such information, and reassess the sufficiency of any safeguards in place to control these risks.

(c) Design and implement safeguards to control the risks you identify through risk assessment, including by:

(1) Implementing and periodically reviewing access controls, including technical and, as appropriate, physical controls to:

(i) Authenticate and permit access only to authorized users to protect against the unauthorized acquisition of customer information; and

(ii) Limit authorized users' access only to customer information that they need to perform their duties and functions, or, in the case of customers, to access their own information;

(2) Identify and manage the data, personnel, devices, systems, and facilities that enable you to achieve business purposes in accordance with their relative importance to business objectives and your risk strategy;

(3) Protect by encryption all customer information held or transmitted by you both in transit over external networks and at rest. To the extent you determine that encryption of customer information, either in transit over external networks or at rest, is infeasible, you may instead secure such customer information using effective alternative compensating controls reviewed and approved by your Qualified Individual;

(4) Adopt secure development practices for in-house developed applications utilized by you for transmitting, accessing, or storing customer information and procedures for evaluating,

assessing, or testing the security of externally developed applications you utilize to transmit, access, or store customer information;

(5) Implement multi-factor authentication for any individual accessing any information system, unless your Qualified Individual has approved in writing the use of reasonably equivalent or more secure access controls;

(6)

(i) Develop, implement, and maintain procedures for the secure disposal of customer information in any format no later than two years after the last date the information is used in connection with the provision of a product or service to the customer to which it relates, unless such information is necessary for business operations or for other legitimate business purposes, is otherwise required to be retained by law or regulation, or where targeted disposal is not reasonably feasible due to the manner in which the information is maintained; and

(ii) Periodically review your data retention policy to minimize the unnecessary retention of data;

(7) Adopt procedures for change management; and

(8) Implement policies, procedures, and controls designed to monitor and log the activity of authorized users and detect unauthorized access or use of, or tampering with, customer information by such users.

(d)

(1) Regularly test or otherwise monitor the effectiveness of the safeguards' key controls, systems, and procedures, including those to detect actual and attempted attacks on, or intrusions into, information systems.

(2) For information systems, the monitoring and testing shall include continuous monitoring or periodic penetration testing and vulnerability assessments. Absent effective continuous monitoring or other systems to detect, on an ongoing basis, changes in information systems that may create vulnerabilities, you shall conduct:

(i) Annual penetration testing of your information systems determined each given year based on relevant identified risks in accordance with the risk assessment; and

(ii) Vulnerability assessments, including any systemic scans or reviews of information systems reasonably designed to identify publicly known security vulnerabilities in your information systems based on the risk assessment, at least every six months; and whenever there are material changes to your operations or business arrangements; and whenever there are circumstances you know or have reason to know may have a material impact on your information security program.

(e) Implement policies and procedures to ensure that personnel are able to enact your information security program by:

(1) Providing your personnel with security awareness training that is updated as necessary to reflect risks identified by the risk assessment;

(2) Utilizing qualified information security personnel employed by you or an affiliate or service provider sufficient to manage your information security risks and to perform or oversee the information security program;

(3) Providing information security personnel with security updates and training sufficient to address relevant security risks; and

(4) Verifying that key information security personnel take steps to maintain current knowledge of changing information security threats and countermeasures.

(f) Oversee service providers, by:

(1) Taking reasonable steps to select and retain service providers that are capable of maintaining appropriate safeguards for the customer information at issue;

(2) Requiring your service providers by contract to implement and maintain such safeguards; and

(3) Periodically assessing your service providers based on the risk they present and the continued adequacy of their safeguards.

(g) Evaluate and adjust your information security program in light of the results of the testing and monitoring required by paragraph (d) of this section; any material changes to your operations or business arrangements; the results of risk assessments performed under paragraph (b)(2) of this section; or any other circumstances that you know or have reason to know may have a material impact on your information security program.

(h) Establish a written incident response plan designed to promptly respond to, and recover from, any security event materially affecting the confidentiality, integrity, or availability of customer information in your control. Such incident response plan shall address the following areas:

(1) The goals of the incident response plan;

(2) The internal processes for responding to a security event;

(3) The definition of clear roles, responsibilities, and levels of decision-making authority;

- (4) External and internal communications and information sharing;
 - (5) Identification of requirements for the remediation of any identified weaknesses in information systems and associated controls;
 - (6) Documentation and reporting regarding security events and related incident response activities; and
 - (7) The evaluation and revision as necessary of the incident response plan following a security event.
- (i) Require your Qualified Individual to report in writing, regularly and at least annually, to your board of directors or equivalent governing body. If no such board of directors or equivalent governing body exists, such report shall be timely presented to a senior officer responsible for your information security program. The report shall include the following information:
- (1) The overall status of the information security program and your compliance with this part; and
 - (2) Material matters related to the information security program, addressing issues such as risk assessment, risk management and control decisions, service provider arrangements, results of testing, security events or violations and management's responses thereto, and recommendations for changes in the information security program.

[86 FR 70307, Dec. 9, 2021]

§ 314.5 Effective date.

Sections 314.4(a), (b)(1), (c)(1) through (8), (d)(2), (e), (f)(3), (h), and (i) are effective as of June 9, 2023.

[87 FR 71510, Nov. 23, 2022]

§ 314.6 Exceptions.

Section 314.4(b)(1), (d)(2), (h), and (i) do not apply to financial institutions that maintain customer information concerning fewer than five thousand consumers.

[86 FR 70308, Dec. 9, 2021]

Florida Administrative Code
69J-128.030 Preamble.

(1) These rules establish standards for developing and implementing administrative, technical and physical safeguards to protect the security, confidentiality, and integrity of customer information, pursuant to Sections 501, 505(b), and 507 of the Gramm-Leach-Bliley Act, codified at 15 U.S.C. 6801, 6805(b) and 6807.

(2)(a) Section 501(a) provides that it is the policy of the Congress that each financial institution has an affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers' nonpublic personal information.

(b) Section 501(b) requires the state insurance regulatory authorities to establish appropriate standards for the financial institutions under their jurisdiction relating to administrative, technical, and physical safeguards:

1. To ensure the security and confidentiality of customer records and information;
2. To protect against any anticipated threats or hazards to the security or integrity of such records; and
3. To protect against unauthorized access to or use of records or information that could result in substantial harm or inconvenience to a customer.

(c) Section 505(b)(2) requires state insurance regulatory authorities to implement the standards prescribed under Section 501(b) by rule with respect to persons engaged in providing insurance.

(d) Section 507 provides, among other things, that a state regulation may afford persons greater privacy protections than those provided by subtitle A of Title V of the Gramm-Leach-Bliley Act.

(3) This Part requires that the safeguards established pursuant to this Part shall apply to nonpublic personal information, including nonpublic personal financial information and nonpublic personal health information.

Rulemaking Authority 624.308(1), 626.9651 FS. Law Implemented 624.307(1), 626.9651 FS. History—New 12-8-02, Formerly 4-128.030, 69B-128.030.

ALTA Best Practice Pillar No. 3

BY MELISSA S. SCALETTA, FUND MEMBER EDUCATION MANAGER

In order to assist Fund Members in preserving their role as title agents in the national lending arena, The Fund has launched an educational campaign concerning the American Land Title Association's (ALTA's) Best Practices. ALTA's Seven Pillars of Best Practices have been a topic discussion at the 2013 Fund Assembly and the most recent *Fund Concept* issues beginning in April 2013. This month we will explore the last pillar, Best Practices Pillar No. 3, concerning privacy and security when dealing with Non-public Personal Information (NPI).

Best Practice Pillar No. 3 requires title agents to **"Adopt and maintain a written privacy and information security program to protect Non-public Personal Information as required by local, state and federal law."** ALTA's Best Practices Framework, referred to as Best Practices 2.0, describes NPI as:

Personally identifiable data such as information provided by a customer on a form or application, information about a customer's transactions, or any other information about a customer which is otherwise unavailable to the general public. NPI includes first name or first initial and last name coupled with any of the following: Social Security Number, driver's license number, state-issued ID number, credit card number, debit card number, or other financial account numbers.

ALTA's Best Practices 2.0 Framework outlines the categories requiring policies and procedures with regard to security and protection of NPI. The procedural areas encompassed within Pillar No. 3 include the following:

Physical Security of NPI. Policy pertaining to physical security of NPI restricts access to NPI to employees who have undergone a background check upon hiring; prohibits or controls the use of removable media; and utilizes secure methods of transmittal of NPI. The physical security policy incorporates requirements that desks are swept clean and documents containing NPI are secured.

Network Security of NPI. Policy governing network security includes guidelines for ensuring secured access and password protection, appropriate use, and

secure collection and use of information technology and NPI. Network security incorporates requirements for strong passwords, use of firewalls and closing electronic files when away from computers.

Disposal of NPI. Policy for disposal of NPI provides for protection against unauthorized access or use.

Disaster Management Plan. Policy documents procedures for notice requirements, interim procedures and return to routine procedures upon reestablishing normalcy in dealing with internal and external security breaches.

Management and Training of Employees in Ensure Compliance. Policy provides for training of employees to recognize and protect NPI, and to execute the firm's policies pertaining to security of NPI. The firm's policies must be known, understood and adopted by employees.

Audit and Oversight of Service Providers. Policy examines and considers the adequacy of the mechanisms by which service providers safeguard NPI.

Notification of Security Breach. Policy includes procedures for notifications to customers and law enforcement agencies of any breach in security.

Not only does the adoption of Best Practices in a manner that is reasonable to your law practice sustain your involvement in real estate closings and the issuance of title insurance, doing so also makes good sense from a business and legal practice prospective. As these Seven Pillars continue to evolve, tools, discussions and guidelines for adoption of Best Practices including the ALTA's Best Practices 2.0 Framework are added for your reference to the Fund's website at www.thefund.com. Several brochures offering guidance specially related to security and protection of NPI are also accessible there. Beginning this November, The Fund will offer legal education web based seminars providing our members and their staff with further information and tools to assist in adoption of ALTA's Best Practices.

trust, separate from the lawyer's property. Retainers are not funds against which future services are billed. Retainers are funds paid to guarantee the future availability of the lawyer's legal services and are earned by the lawyer on receipt. Retainers, being funds of the lawyer, may not be placed in the client's trust account.

The test of excessiveness found elsewhere in the Rules Regulating The Florida Bar applies to all fees for legal services including retainers, nonrefundable retainers, and minimum or flat fees.

Amended July 20, 1989, effective Oct. 1, 1989 (547 So.2d 117); Oct. 10, 1991, effective Jan. 1, 1992 (587 So.2d 1121); July 23, 1992, effective Jan. 1, 1993 (605 So.2d 252); July 1, 1993 (621 So.2d 1032); July 20, 1995 (658 So.2d 930); April 24, 1997 (692 So.2d 181); June 14, 2001, effective July 14, 2001 (797 So.2d 551); April 25, 2002 (820 So.2d 210); May 20, 2004 (SC03-705) (875 So.2d 448); March 23, 2006, effective May 22, 2006 (SC04-2246), (933 So.2d 417); December 20, 2007, effective March 1, 2008 (SC06-736), (978 So.2d 91); November 19, 2009, effective February 1, 2010 (SC08-1890) (34 Fla.L.Weekly S628a); amended July 7, 2011, effective October 1, 2011 (SC10-1968). Amended June 11, 2015, effective October 1, 2015 (SC14-2088), amended November 9, 2017, effective February 1, 2018.

RULE 5-1.2 TRUST ACCOUNTING RECORDS AND PROCEDURES

(a) Applicability. The provisions of these rules apply to all trust funds received or disbursed by members of The Florida Bar in the course of their professional practice of law as members of The Florida Bar except special trust funds received or disbursed by a lawyer as guardian, personal representative, receiver, or in a similar capacity such as trustee under a specific trust document where the trust funds are maintained in a segregated special trust account and not the general trust account and where this special trust position has been created, approved, or sanctioned by law or an order of a court that has authority or duty to issue orders pertaining to maintenance of such special trust account. These rules apply to matters in which a choice of laws analysis indicates that such matters are governed by the laws of Florida.

As set forth in this rule, "lawyer" denotes a person who is a member of The Florida Bar or otherwise authorized to practice in any court of the state of Florida. "Law firm" denotes a lawyer or lawyers in a private firm who handle client trust funds.

(b) Minimum Trust Accounting Records. Records may be maintained in their original format or stored in digital media as long as the copies include all data contained in the original documents and may be produced when required. The following are the minimum trust accounting records that must be maintained:

(1) a separate bank or savings and loan association account or accounts in the name of the lawyer or law firm and clearly labeled and designated as a "trust account";

(2) original or clearly legible copies of deposit slips if the copies include all data on the originals and, in the case of currency or coin, an additional cash receipts book, clearly identifying the date and source of all trust funds received and the client or matter for which the funds were received;

(3) original canceled checks or clearly legible copies of original canceled checks for all funds disbursed from the trust account, all of which must:

(A) be numbered consecutively

(B) include all endorsements and all other data and tracking information, and

(C) clearly identify the client or case by number or name in the memo area of the check;

(4) other documentary support for all disbursements and transfers from the trust account including records of all electronic transfers from client trust accounts, including:

(A) the name of the person authorizing the transfer;

(B) the name of the recipient;

(C) confirmation from the banking institution confirming the number of the trust account from which money is withdrawn; and

(D) the date and time the transfer was completed;

(5) original or clearly legible digital copies of all records regarding all wire transfers into or out of the trust account, which at a minimum must include the receiving and sending financial institutions' ABA routing numbers and names, and the receiving and sending account holder's name, address and account number. If the receiving financial institution processes through a correspondent or intermediary bank, then the records must include the ABA routing number and name for the intermediary bank. The wire transfer information must also include the name of the client or matter for which the funds were transferred or received, and the purpose of the wire transfer, (e.g., "payment on invoice 1234" or "John Doe closing").

(6) a separate cash receipts and disbursements journal, including columns for receipts, disbursements, transfers, and the account balance, and containing at least:

(A) the identification of the client or matter for which the funds were received, disbursed, or transferred;

(B) the date on which all trust funds were received, disbursed, or transferred;

(C) the check number for all disbursements; and

(D) the reason for which all trust funds were received, disbursed, or transferred;

(7) a separate file or ledger with an individual card or page for each client or matter, showing all individual receipts, disbursements, or transfers and any unexpended balance, and containing:

(A) the identification of the client or matter for which trust funds were received, disbursed, or transferred;

(B) the date on which all trust funds were received, disbursed, or transferred;

(C) the check number for all disbursements; and

(D) the reason for which all trust funds were received, disbursed, or transferred;
and

(8) all bank or savings and loan association statements for all trust accounts.

(c) Responsibility of Lawyers for Firm Trust Accounts and Reporting.

(1) Every law firm with more than 1 lawyer must have a written plan in place for supervision and compliance with this rule for each of the firm's trust account(s), which plan must be disseminated to each lawyer in the firm. The written plan must include the name(s) of the signatories for the law firm's trust accounts, the name(s) of the lawyer(s) who are responsible for reconciliation of the law firm's trust account(s) monthly and annually and the name(s) of the lawyer(s) who are responsible for answering any questions that lawyers in the firm may have about the firm's trust account(s). This written plan must be updated and re-issued to each lawyer in the firm whenever there are material changes to the plan, such as a change in the trust account signatories and/or lawyer(s) responsible for reconciliation of the firm's trust account(s).

(2) Every lawyer is responsible for that lawyer's own actions regarding trust account funds subject to the requirements of chapter 4 of these rules. Any lawyer who has actual knowledge that the firm's trust account(s) or trust accounting procedures are not in compliance with chapter 5 may report the noncompliance to the managing partner or shareholder of the lawyer's firm. If the noncompliance is not corrected within a reasonable time, the lawyer must report the noncompliance to staff counsel for the bar if required to do so pursuant to the reporting requirements of chapter 4.

(d) Minimum Trust Accounting Procedures. The minimum trust accounting procedures that must be followed by all members of The Florida Bar (when a choice of laws analysis indicates that the laws of Florida apply) who receive or disburse trust money or property are as follows:

(1) The lawyer is required to make **monthly:**

(A) **reconciliations** of all trust bank or savings and loan association accounts, disclosing the balance per bank, deposits in transit, outstanding checks identified by date and check number, and any other items necessary to reconcile the balance per bank with the balance per the checkbook and the cash receipts and disbursements journal;
and

(B) a **comparison** between the total of the reconciled balances of all trust accounts and the total of the trust ledger cards or pages, together with specific descriptions of any differences between the 2 totals and reasons for these differences.

(2) The lawyer is required to **prepare an annual detailed list identifying the balance of the unexpended trust money held for each client or matter.**

(3) **The above reconciliations, comparisons, and listings must be retained for at least 6 years.**

(4) The lawyer or law firm must authorize, at the time the account is opened, and request any bank or savings and loan association where the lawyer is a signatory on a trust account to notify Staff Counsel, The Florida Bar, 651 East Jefferson Street, Tallahassee, Florida 32399-2300, in the event the account is overdrawn or any trust check is dishonored or returned due to insufficient funds or uncollected funds, absent bank error.

(5) The lawyer must file with The Florida Bar between June 1 and August 15 of each year a trust accounting certificate showing compliance with these rules on a form approved by the board of governors. If the lawyer fails to file the trust accounting certificate, the lawyer will be deemed a delinquent member and ineligible to practice law.

(e) Electronic Wire Transfers. Authorized electronic transfers from a lawyer or law firm's trust account are limited to:

- (1) money required to be paid to a client or third party on behalf of a client;
- (2) expenses properly incurred on behalf of a client, such as filing fees or payment to third parties for services rendered in connection with the representation;
- (3) money transferred to the lawyer for fees which are earned in connection with the representation and which are not in dispute; or
- (4) money transferred from one trust account to another trust account.

(f) Record Retention. A lawyer or law firm that receives and disburses client or third-party funds or property must maintain the records required by this chapter for 6 years subsequent to the final conclusion of each representation in which the trust funds or property were received.

(1) On dissolution of a law firm or of any legal professional corporation, the partners shall make reasonable arrangements for the maintenance and retention of client trust account records specified in this rule.

(2) On the sale of a law practice, the seller must make reasonable arrangements for the maintenance and retention of trust account records specified in this rule consistent with other requirements regarding the sale of a law firm set forth in Chapter 4 of these rules.

(g) Audits. Any of the following are cause for The Florida Bar to order an audit of a trust account:

- (1) failure to file the trust account certificate required by this rule;
- (2) report of trust account violations or errors to staff counsel under this rule;
- (3) return of a trust account check for insufficient funds or for uncollected funds, absent bank error;
- (4) filing of a petition for creditor relief on behalf of a lawyer;
- (5) filing of felony charges against a lawyer;
- (6) adjudication of insanity or incompetence or hospitalization of a lawyer under The Florida Mental Health Act;
- (7) filing of a claim against a lawyer with the Clients' Security Fund;
- (8) request by the chair or vice chair of a grievance committee or the board of governors;
- (9) on court order; or
- (10) on entry of an order of disbarment, on consent or otherwise.

(h) Cost of Audit. Audits conducted in any of the circumstances enumerated in this rule will be at the cost of the lawyer audited only when the audit reveals that the lawyer was not in substantial compliance with the trust accounting requirements. It will be the obligation of any lawyer who is being audited to produce all records and papers concerning property and funds held in trust and to provide such explanations as may be required for the audit. Records of general accounts are not required to be produced except to verify that trust money has not been deposited in them. If it has been determined that trust money has been deposited into a general account, all of the transactions pertaining to any firm account will be subject to audit.

(i) Failure to Comply With Subpoena for Trust Accounting Records. Failure of a member to timely produce trust accounting records will be considered as a matter of contempt and process in the manner provided in subdivision (d) and (f) of rule 3-7.11, Rules Regulating The Florida Bar.

Amended Oct. 10, 1991, effective Jan. 1, 1992 (587 So.2d 1121); July 23, 1992, effective Jan. 1, 1993 (605 So.2d 252); July 17, 1997 (697 So.2d 115); April 25, 2002 (820 So.2d 210); July 3, 2003 (850 So.2d 499); May 20, 2004 (SC03-705) (875 So.2d 448); November 19, 2009, effective February 1, 2010 (SC08-1890) (34 Fla.L.Weekly S628a). Amended April 12, 2012, effective July 1, 2012 (SC10-1967); amended May 29, 2014, effective June 1, 2014 (SC12-2234). Amended June 11, 2015, effective October 1, 2015 (SC14-2088), amended November 9, 2017, effective February 1, 2018.

CHAPTER 5. RULES REGULATING TRUST ACCOUNTS

5-1. GENERALLY

RULE 5-1.1 TRUST ACCOUNTS

(a) Nature of Money or Property Entrusted to Attorney.

(1) *Trust Account Required; Location of Trust Account; Commingling Prohibited.* A lawyer must hold in trust, separate from the lawyer's own property, funds and property of clients or third persons that are in a lawyer's possession in connection with a representation. All funds, including advances for fees, costs, and expenses, must be kept in a separate federally insured bank, credit union, or savings and loan association account maintained in the state where the lawyer's office is situated or elsewhere with the consent of the client or third person and clearly labeled and designated as a trust account except:

(A) A lawyer may maintain funds belonging to the lawyer in the lawyer's trust account in an amount no more than is reasonably sufficient to pay bank charges relating to the trust account; and

(B) A lawyer may deposit the lawyer's own funds into trust to replenish a shortage in the lawyer's trust account. Any deposits by the lawyer to cover trust account shortages must be no more than the amount of the trust account shortage, but may be less than the amount of the shortage. The lawyer must notify the bar's lawyer regulation department immediately of the shortage in the lawyer's trust account, the cause of the shortage, and the amount of the replenishment of the trust account by the lawyer.

(2) *Compliance with Client Directives.* Trust funds may be separately held and maintained other than in a bank, credit union, or savings and loan association account if the lawyer receives written permission from the client to do so and provided that written permission is received before maintaining the funds other than in a separate account.

(3) *Safe Deposit Boxes.* If a lawyer uses a safe deposit box to store trust funds or property, the lawyer must advise the institution in which the deposit box is located that it may include property of clients or third persons.

(b) Application of Trust Funds or Property to Specific Purpose. Money or other property entrusted to a lawyer for a specific purpose, including advances for fees, costs, and expenses, is held in trust and must be applied only to that purpose. Money and other property of clients coming into the hands of a lawyer are not subject to counterclaim or setoff for attorney's fees, and a refusal to account for and deliver over the property on demand is conversion.

(c) Liens Permitted. This subchapter does not preclude the retention of money or other property on which the lawyer has a valid lien for services nor does it preclude the payment of agreed fees from the proceeds of transactions or collection.

(d) Controversies as to Amount of Fees. Controversies as to the amount of fees are not grounds for disciplinary proceedings unless the amount demanded is clearly excessive, extortionate, or fraudulent. In a controversy alleging a clearly excessive, extortionate, or fraudulent fee, announced willingness of an attorney to submit a dispute as to the amount of a fee to a competent tribunal for determination may be considered in any determination as to intent or in mitigation of discipline; provided, such willingness shall not preclude admission of any other relevant admissible evidence relating to such controversy, including evidence as to the withholding of funds or property of the client, or to other injury to the client occasioned by such controversy.

(e) Notice of Receipt of Trust Funds; Delivery; Accounting. On receiving funds or other property in which a client or third person has an interest, a lawyer must promptly notify the client or third person. Except as stated in this rule or otherwise permitted by law or by agreement with the client, a lawyer must promptly deliver to the client or third person any funds or other property that the client or third person is entitled to receive and, on request by

the client or third person, must promptly render a full accounting regarding the property.

(f) Disputed Ownership of Trust Funds. When in the course of representation a lawyer is in possession of property in which 2 or more persons (1 of whom may be the lawyer) claim interests, the property must be treated by the lawyer as trust property, but the portion belonging to the lawyer or law firm must be withdrawn within a reasonable time after it becomes due unless the right of the lawyer or law firm to receive it is disputed, in which event the portion in dispute must be kept separate by the lawyer until the dispute is resolved. The lawyer must promptly distribute all portions of the property as to which the interests are not in dispute.

(g) Interest on Trust Accounts (IOTA) Program.

(1) *Definitions.* As used in this rule, the term:

(A) “Nominal or short term” describes funds of a client or third person that the lawyer has determined cannot earn income for the client or third person in excess of the costs to secure the income.

(B) “Foundation” means The Florida Bar Foundation, Inc. which serves as the designated IOTA fund administrator and monitors and receives IOTA funds from eligible institutions and distributes IOTA funds consistent with the obligations and directives in this rule.

(C) “IOTA account” means an interest or dividend-bearing trust account benefiting The Florida Bar Foundation established in an eligible institution for the deposit of nominal or short-term funds of clients or third persons.

(D) “Eligible institution” means any bank or savings and loan association authorized by federal or state laws to do business in Florida and insured by the Federal Deposit Insurance Corporation, any state or federal credit union authorized by federal or state laws to do business in Florida and insured by the National Credit Union Share Insurance Fund, or any successor insurance corporation(s) established

by federal or state laws, or any open-end investment company registered with the Securities and Exchange Commission and authorized by federal or state laws to do business in Florida, all of which must meet the requirements set out in subdivision (5), below.

(E) “Interest or dividend-bearing trust account” means a federally insured checking account, business or consumer deposit account or sub account, business or consumer deposit account or sub account that does not have a maturity date (non-maturing deposit), or investment product, including a daily financial institution repurchase agreement or a money market fund. A daily financial institution repurchase agreement must be fully collateralized by, and an open-end money market fund must consist solely of, United States Government Securities. A daily financial institution repurchase agreement may be established only with an eligible institution that is deemed to be “well capitalized” or “adequately capitalized” as defined by applicable federal statutes and regulations. An open-end money market fund must hold itself out as a money market fund as defined by applicable federal statutes and regulations under the Investment Company Act of 1940 and have total assets of at least \$250 million. The funds covered by this rule are subject to withdrawal on request and without delay.

(F) A “qualified grantee organization” is a charitable or other nonprofit organization that facilitates or directly provides qualified legal services by qualified legal services providers and that has experience in successfully doing so.

(G) “Qualified legal services” are free legal services provided directly to low-income clients for their civil legal needs in Florida, and includes post-conviction representation, programs that assist low-income clients in navigating legal processes, and the publication of legal forms or other legal resources for use by pro se litigants.

(H) A “qualified legal services provider” is a member of The Florida Bar or other individual authorized by the Rules

Title XXXVII

INSURANCE

Chapter 627

INSURANCE RATES AND CONTRACTS

[View Entire Chapter](#)

627.7845 Determination of insurability required; preservation of evidence of title search and examination.—

(1) A title insurer may not issue a title insurance commitment, endorsement, or title insurance policy until the title insurer has caused to be made a determination of insurability based upon the evaluation of a reasonable title search or a search of the records of a Uniform Commercial Code filing office, as applicable, has examined such other information as may be necessary, and has caused to be made a determination of insurability of title or the existence, attachments, perfection, and priority of a Uniform Commercial Code security interest, including endorsement coverages, in accordance with sound underwriting practices.

(2) The title insurer shall cause the evidence of the determination of insurability and the reasonable title search or search of the records of a Uniform Commercial Code filing office to be preserved and retained in its files or in the files of its title insurance agent or agency for at least 7 years after the title insurance commitment or title insurance policy was issued. The title insurer or its agent or agency must produce the evidence required to be maintained under this subsection at its offices upon the demand of the office. Instead of retaining the original evidence, the title insurer or its agent or agency may, in the regular course of business, establish a system under which all or part of the evidence is recorded, copied, or reproduced by any photographic, photostatic, microfilm, microcard, miniature photographic, or other process that accurately reproduces or forms a durable medium for reproducing the original.

(3) The title insurer or its agent or agency must maintain a record of the actual premium charged for issuance of the policy and any endorsements in its files for a period of not less than 7 years. The title insurer, agent, or agency must produce the record at its office upon demand of the office.

(4) This section does not apply to an insurer assuming no primary liability in a contract of reinsurance or to an insurer acting as a coinsurer if any other coinsuring insurer has complied with this section.

History.—ss. 582, 809(2nd), ch. 82-243; s. 79, ch. 82-386; s. 4, ch. 85-185; ss. 102, 114, ch. 92-318; s. 18, ch. 99-286; s. 1207, ch. 2003-261; s. 3, ch. 2005-153; s. 7, ch. 2007-44; s. 13, ch. 2014-112.



K. Perform such services and render such assistance as Insurer may reasonably request in connection with: (i) any regulatory examination, information request or data call, or (ii) any claim or litigation arising from: (a) a commitment, policy, endorsement or other Title Insurance Product issued by Agent or by Insurer on behalf of Agent, or (b) any conduct of Agent. Such services and assistance shall be performed by Agent regardless whether such examination, information request, data call, claim or litigation is instituted during the term of this Agreement or following the termination of this Agreement. In addition, Agent will promptly forward to Insurer:

(i) All documents received by Agent in which Insurer is a party to any administrative and/or judicial proceedings;

(ii) All written complaints or inquiries made to any regulatory agency regarding transactions involving Title Insurance Products of Insurer; and

(iii) All original documentation and work papers associated with the transaction or conduct giving rise to any examination, claim or complaint;

L. Maintain and preserve (by paper or electronic means) all records, books, books of account, files, documents, correspondence, bank records, title evidence and material of all kinds relating to Agent's Title Insurance Business for the time period required by the Laws, but in no event for a period of less than ten (10) years; and

M. Notify Insurer immediately of the following:

(i) Any claims involving Title Insurance Products. Agent will provide Insurer with all documentation received by Agent in connection with the claim;

(ii) Any request, subpoena, or legal process for information or documentation received by Agent from any state or federal government, judicial or regulatory authority. If the request, subpoena or legal process is directed to Agent, Agent will promptly comply with the request, subpoena or legal process by the applicable date set forth therein, and provide a copy of the response to Insurer;

(iii) Agent becomes unable, for any reason, to continue conducting Agent's Title Insurance Business;

(iv) Any change in the ownership of Agent of more than a twenty-five (25%) interest;

(v) Any change in Validating Officers or other key officers or employees of Agent. In the event that such a change occurs, Agent will promptly provide to Insurer a fully executed "Disclosure & Release of Information Authorization." Agent will also undertake all actions necessary to assure the insurance coverages required in Section 12 are maintained at all times;

(vi) Any change in the location of Agent's principal office or opening, closing or changing the location of any of its other offices;

(vii) Any criminal or civil action in which Agent is a defendant; and

(viii) Any shortage in any of Agent's escrow or trust accounts.

5. INSURER'S DUTIES

Insurer will:

A. Provide Agent with the Title Insurance Products and a means of accounting for them;

B. Provide Agent with the Underwriting Materials; and

§ 1024.10 One-day advance inspection of HUD-1 or HUD-1A settlement statement; delivery; recordkeeping.

THIS VERSION IS THE CURRENT REGULATION

- [View all versions of this regulation](#)
- [Search this regulation](#)

Regulation X

§ 1024.10(e)

(a) **Inspection one day prior to settlement upon request by the borrower.** The settlement agent shall permit the borrower to inspect the HUD-1 or HUD-1A settlement statement, completed to set forth those items that are known to the settlement agent at the time of inspection, during the business day immediately preceding settlement. Items related only to the seller's transaction may be omitted from the HUD-1.

(b) **Delivery.** The settlement agent shall provide a completed HUD-1 or HUD-1A to the borrower, the seller (if there is one), the lender (if the lender is not the settlement agent), and/or their agents. When the borrower's and seller's copies of the HUD-1 or HUD-1A differ as permitted by the instructions in appendix A to this part, both copies shall be provided to the lender (if the lender is not the settlement agent). The settlement agent shall deliver the completed HUD-1 or HUD-1A at or before the settlement, except as provided in paragraphs (c) and (d) of this section.

(c) **Waiver.** The borrower may waive the right to delivery of the completed HUD-1 or HUD-1A no later than at settlement by executing a written waiver at or before settlement. In such case, the completed HUD-1 or HUD-1A shall be mailed or delivered to the borrower, seller, and lender (if the lender is not the settlement agent) as soon as practicable after settlement.

(d) **Exempt transactions.** When the borrower or the borrower's agent does not attend the settlement, or when the settlement agent does not conduct a meeting of the parties for that purpose, the transaction shall be exempt from the requirements of paragraphs (a) and (b) of this section, except that the HUD-1 or HUD-1A shall be mailed or delivered as soon as practicable after settlement.

(e) **Recordkeeping.** The lender shall retain each completed HUD-1 or HUD-1A and related documents for five years after settlement, unless the lender disposes of its interest in the mortgage and does not service the mortgage. In that case, the lender shall provide its copy of the HUD-1 or HUD-1A to the owner or servicer of the mortgage as a part of the transfer of the loan file. Such owner or servicer shall retain the HUD-1 or HUD-1A for the remainder of the five-year period. The Bureau shall have the right to inspect or require copies of records covered by this paragraph (e).

§ 1026.25 Record retention.

THIS VERSION IS THE CURRENT REGULATION

- [View all versions of this regulation](#)
- [Search this regulation](#)

Regulation Z

[§ 1026.25\(c\)\(2\)\(ii\)](#)

(a) General rule. A creditor shall retain evidence of compliance with this part (other than advertising requirements under §§ [1026.16](#) and 1026.24, and other than the requirements under § [1026.19\(e\)](#) and (f)) for two years after the date disclosures are required to be made or action is required to be taken. The administrative agencies responsible for enforcing the regulation may require creditors under their jurisdictions to retain records for a longer period if necessary to carry out their enforcement responsibilities under section 108 of the Act.

Official interpretation of 25(a) General Rule

(b) Inspection of records. A creditor shall permit the agency responsible for enforcing this part with respect to that creditor to inspect its relevant records for compliance.

(c) Records related to certain requirements for mortgage loans —

Official interpretation of 25(c) Records Related to Certain Requirements for Mortgage Loans.

(1) Records related to requirements for loans secured by real property or a cooperative unit —

(i) General rule. Except as provided under paragraph (c)(1)(ii) of this section, a creditor shall retain evidence of compliance with the requirements of § [1026.19\(e\)](#) and (f) for three years after the later of the date of consummation, the date disclosures are required to be made, or the date the action is required to be taken.

(ii) Closing disclosures.

(A) A creditor shall retain each completed disclosure required under § [1026.19\(f\)\(1\)\(i\)](#) or (f)(4)(i), and all documents related to such disclosures, for five years after consummation, notwithstanding paragraph (c)(1)(ii)(B) of this section.

(B) If a creditor sells, transfers, or otherwise disposes of its interest in a mortgage loan subject to § [1026.19\(f\)](#) and does not service the mortgage loan, the creditor shall provide a copy of the disclosures required under § [1026.19\(f\)\(1\)\(i\)](#) or (f)(4)(i) to the owner or servicer of the mortgage as a part of the transfer of the loan file. Such owner or servicer shall retain such disclosures for the remainder of the five-year period described under paragraph (c)(1)(ii)(A) of this section.

(C) The Bureau shall have the right to require provision of copies of records related to the disclosures required under § [1026.19\(f\)\(1\)\(i\)](#) and (f)(4)(i).

(2) Records related to requirements for loan originator compensation. Notwithstanding paragraph (a) of this section, for transactions subject to § [1026.36](#):

Official interpretation of 25(c)(2) Records Related to Requirements for Loan Originator Compensation

(i) A creditor shall maintain records sufficient to evidence all compensation it pays to a loan originator, as defined in § [1026.36\(a\)\(1\)](#), and the compensation agreement that governs those payments for three years after the date of payment.

(ii) A loan originator organization, as defined in § [1026.36\(a\)\(1\)\(iii\)](#), shall maintain records sufficient to evidence all compensation it receives from a creditor, a consumer, or another person; all compensation it pays to any individual loan originator, as defined in § [1026.36\(a\)\(1\)\(ii\)](#); and the compensation agreement that governs each such receipt or payment, for three years after the date of each such receipt or payment.

(3) Records related to minimum standards for transactions secured by a dwelling. Notwithstanding paragraph (a) of this section, a creditor shall retain evidence of compliance with § [1026.43](#) of this regulation for three years after consummation of a transaction covered by that section.

Official interpretation of 25(c)(3) Records related to minimum standards for transactions secured by a dwelling.

26 CFR § 1.1445-2 - Situations in which withholding is not required under section 1445(a).

- [CFR](#)
- [Table of Popular Names](#)

[prev](#) | [next](#)

§ 1.1445-2 Situations in which [withholding](#) is not required under section 1445(a).

(a) Purpose and scope of section. This section provides rules concerning various situations in which withhold is not required under section 1445(a). In general, a [transferee](#) has a duty to withhold under section 1445(a) only if both of the following are true:

- (1) The transferor is a [foreign person](#); and
- (2) The [transferee](#) is [acquiring](#) a U.S. [real property interest](#).

Thus, paragraphs [\(b\)](#) and [\(c\)](#) of this section provide rules under which a [transferee](#) of [property](#) can ascertain that he has no duty to withhold because one or the other of the two key elements is missing. Under paragraph [\(b\)](#), a [transferee](#) may determine that no [withholding](#) is required because the transferor is not a [foreign person](#). Under paragraph [\(c\)](#), a [transferee](#) may determine that no [withholding](#) is required because the [property acquired](#) is not a U.S. [real property interest](#). Finally, [paragraph \(d\)](#) of this section provides rules concerning [exceptions](#) to the [withholding requirement](#).

(b) Transferor not a foreign person—(1) *In general.* No [withholding](#) is required under section 1445 if the transferor of a U.S. [real property interest](#) is not a [foreign person](#). Therefore, [paragraph \(b\)\(2\)](#) of this section provides rules pursuant to which the transferor can provide a [certification](#) of non-foreign status to inform the [transferee](#) that [withholding](#) is not required. A [transferee](#) that obtains such a [certification](#) must retain that document for five years, as provided in [paragraph \(b\)\(3\)](#) of this section. Except to the extent provided in [paragraph \(b\)\(4\)](#) of this section, the obtaining of this [certification](#) excuses the [transferee](#) from any [liability](#) otherwise imposed by section 1445 and § 1.1445–1(e). However, section 1445 and the rules of this section do not impose any [obligation](#) upon a [transferee](#) to obtain a [certification](#) from the transferor, thus, a [transferee](#) may instead rely upon other means to ascertain the non-foreign status of the transferor. If, however, the [transferee](#) relies upon other means and the transferor was, in fact, a [foreign person](#), then the [transferee](#) is subject to the [liability](#) imposed by section 1445 and § 1.1445–1(e).

A [transferee](#) is in no event required to rely upon other means to ascertain the non-foreign status of the transferor and may demand a [certification](#) of non-foreign status. If the [certification](#) is not provided, the [transferee](#) may withhold tax under section 1445 and will be considered, for purposes of sections 1461 through 1463, to have been required to withhold such tax.

(2) Transferor's certification of non-foreign status—(i) *In general.* The rules in this paragraph [\(b\)\(2\)\(i\)](#) apply for purposes of the transferor's [certification](#) of non-foreign status (including a [certification](#) of non-foreign status provided by a [withholding](#) qualified [holder](#) (as defined in § 1.1445–1(g)(11)).

(A) A [transferee](#) of a U.S. [real property interest](#) is not required to withhold under section 1445(a) if, before or at the time of the [transfer](#), the transferor furnishes to the [transferee](#) a [certification](#) that is signed under [penalties](#) of perjury and—

(I) [States](#) that the transferor is not a [foreign person](#); and

(2) Sets forth the transferor's [name](#), [identifying number](#) and home address (in the case of an individual) or office address (in the case of an entity).

(B) For purposes of [paragraph \(b\)\(2\)\(i\)\(A\)](#) of this section, a [foreign person](#) is a [nonresident alien](#) individual, [foreign corporation](#), foreign [partnership](#), [foreign trust](#), or foreign estate, except that a [withholding](#) qualified [holder](#) (as defined in § 1.1445–1(g)(11)) is not a [foreign person](#). Additionally, a [foreign corporation](#) that has made a valid [election](#) under section 897(i) is generally not treated as a [foreign person](#) for purposes of section 1445. In this regard, see § 1.1445–7. Pursuant to § 1.897–1(p), an individual's [identifying number](#) is the individual's Social [Security](#) number and any other [person's](#) [identifying number](#) is its U.S. [employer identification number](#) (EIN), or, if the transferor is a [withholding](#) qualified [holder](#) (as defined in § 1.1445–1(g)(11)) that does not have a U.S. [taxpayer identification](#) number, a foreign tax [identification](#) number [issued](#) by its jurisdiction of residence. A [certification](#) pursuant to this paragraph (b) must be verified as true and signed under [penalties](#) of perjury by a [responsible officer](#) in the case of a [corporation](#), by a general [partner](#) in the case of a [partnership](#), and by a [trustee](#), executor, or equivalent [fiduciary](#) in the case of a [trust](#) or estate. No particular form is needed for a [certification](#) pursuant to this paragraph (b), nor is any particular language required, so long as the document meets the [requirements](#) of this paragraph (b)(2)(i), except that, with respect to a [certification](#) submitted by a [withholding](#) qualified [holder](#) (as defined in § 1.1445–1(g)(11)), the transferor must [state](#) on the [certification](#) that it is treated as a non-foreign [person](#) because it is a [withholding](#) qualified [holder](#) and must further specify whether it qualifies as a [withholding](#) qualified [holder](#) because it is a qualified [holder](#) under § 1.897(l)–1(d) or a foreign [partnership](#) that satisfies the [requirements](#) of § 1.1445–1(g)(11). Samples of acceptable [certifications](#) are provided in [paragraph \(b\)\(2\)\(iv\)](#) of this section.

(ii) *Foreign corporation that “has made election under section 897(i).* A [foreign corporation](#) that has made a valid [election](#) under section 897(i) to be treated as a [domestic corporation](#) for purposes of section 897 may provide a [certification](#) of non-foreign status pursuant to this paragraph (b)(2). However, an electing [foreign corporation](#) must attach to such [certification](#) a copy of the acknowledgment of the [election](#) provided to the [corporation](#) by the Internal Revenue Service pursuant to § 1.897–3(d)(4).

An acknowledgment is valid for this purpose only if it [states](#) that the information required by § 1.897–3 has been determined to be complete.

(iii) *Disregarded entities.* A [disregarded entity](#) may not certify that it is the transferor of a U.S. [real property interest](#), as the [disregarded entity](#) is not the transferor for U.S. tax purposes, including sections 897 and 1445. Rather, the [owner](#) of the [disregarded entity](#) is treated as the transferor of [property](#) and must provide a certificate of non-foreign status to avoid [withholding](#) under section 1445. A [disregarded entity](#) for these purposes means an [entity](#) that is disregarded as an [entity](#) separate from its [owner](#) under § 301.7701–3 of this chapter, a qualified REIT [subsidiary](#) as defined in section 856(i), or a qualified subchapter S [subsidiary](#) under section 1361(b)(3)(B). Any [domestic entity](#) must include in its [certification](#) of non-foreign status with respect to the [transfer](#) a [certification](#) that it is not a [disregarded entity](#). This paragraph (b)(2)(iii) and the sample [certification](#) provided in [paragraph \(b\)\(2\)\(iv\)\(B\)](#) of this section (to the extent it addresses disregarded entities) is applicable for [dispositions](#) occurring September 4, 2003.

(iv) Sample certifications—(A) Individual transferor.

“Section 1445 of the [Internal Revenue Code](#) provides that a [transferee](#) (buyer) of a U.S. [real property interest](#) must withhold tax if the transferor (seller) is a [foreign person](#). To inform the [transferee](#) (buyer) that [withholding](#) of tax is not required upon my [disposition](#) of a U.S. [real property interest](#), I, [name of transferor], hereby certify the following:

1. I am not a [nonresident alien](#) for purposes of U.S. [income](#) taxation;
2. My U.S. [taxpayer identifying number](#) [Social [Security](#) number] is ____; and
3. My home address is:

I understand that this [certification](#) may be disclosed to the Internal Revenue Service by the [transferee](#) and that any false [statement](#) I have made here could be punished by fine, imprisonment, or both.

Under [penalties](#) of perjury I declare that I have examined this [certification](#) and to the best of my knowledge and belief it is true, correct, and complete. [Signature and Date]”

(B) Entity transferor.

“Section 1445 of the [Internal Revenue Code](#) provides that a [transferee](#) of a U.S. [real property interest](#) must withhold tax if the transferor is a [foreign person](#). For U.S. tax purposes (including section 1445), the [owner](#) of a [disregarded entity](#) (which has legal title to a U.S. [real property interest](#) under local law) will be the transferor of the [property](#) and not the [disregarded entity](#). To inform the [transferee](#) that [withholding](#) of tax is not required upon the [disposition](#) of a U.S. [real property interest](#) by [name of transferor], the undersigned hereby certifies the following on behalf of [name of the transferor]:

1. [Name of transferor] is not a [foreign corporation](#), foreign [partnership](#), [foreign trust](#), or foreign estate (as those [terms](#) are defined in the [Internal Revenue Code](#) and [Income](#) Tax Regulations);
2. [Name of transferor] is not a [disregarded entity](#) as defined in § 1.1445–2(b)(2)(iii);
3. [Name of transferor]’s U.S. [employer identification number](#) is ____; and
4. [Name of transferor]’s office address is _____.

[Name of transferor] understands that this [certification](#) may be disclosed to the Internal Revenue Service by [transferee](#) and that any false [statement](#) contained herein could be punished by fine, imprisonment, or both.

Under [penalties](#) of perjury I declare that I have examined this [certification](#) and to the best of my knowledge and belief it is true, correct, and complete, and I further declare that I have authority to sign this document on behalf of [name of transferor].

[Signature(s) and date]

[Title(s)]”

(v) Form W–9. For purposes of paragraph (b)(2)(i) of this section, a [certification](#) of non-foreign status includes a valid Form W–9, *Request for Taxpayer Identification Number and Certification*, or its [successor](#), submitted to the [transferee](#) by the transferor.

(vi) Form W–8EXP. A [certification](#) of non-foreign status may be made by a [withholding](#) qualified [holder](#) (as defined under § 1.1445–1(g)(11)) as provided in paragraph (b)(2)(i) of this section to certify its qualified [holder](#) status. A [certification](#) of non-foreign status under paragraph (b)(2)(i) of this section also includes a [certification](#) made on a Form W–8EXP (or its successor) that [states](#) that the transferor is treated as a non-foreign [person](#) because it is a [withholding](#) qualified [holder](#) and must further specify whether it qualifies as

a [withholding](#) qualified [holder](#) because it is a qualified [holder](#) under § 1.897(l)–1(d) or a foreign [partnership](#) that satisfies the [requirements](#) of § 1.1445–1(g)(11). The [certification](#) must also meet all of the [other requirements](#) for a valid Form W–8EXP (or its successor) as provided on the form and the instructions to the form. A qualified [holder](#) may not provide a [certification](#) of non-foreign status on a Form W–9 (or its successor) as permitted in [paragraph \(b\)\(2\)\(v\)](#) of this section.

(3) *Transferee must retain certification.* If a [transferee](#) obtains a transferor's [certification](#) pursuant to the rules of this paragraph (b), then the [transferee](#) must retain that [certification](#) until the end of the fifth [taxable year](#) following the [taxable year](#) in which the transfer takes place. The [transferee](#) must retain the [certification](#), and make it available to the Internal Revenue Service when requested in accordance with the [requirements](#) of section 6001 and regulations thereunder.

(4) *Reliance upon certification not permitted*—(i) *In general.* A [transferee](#) may not rely upon a transferor's [certification](#) pursuant to this paragraph (b) under the circumstances set forth in either subdivision (ii) or (iii) of this paragraph (b)(4). In either of those circumstances, a [transferee's](#) [withholding obligation](#) shall apply as if a [certification](#) had never been obtained, and the [transferee](#) is fully liable pursuant to section 1445 and § 1.1445–1(e) for any failure to withhold.

(ii) *Failure to attach IRS acknowledgment of election.* A [transferee](#) that knows that the transferor is a [foreign corporation](#) may not rely upon a [certification](#) of non-foreign status provided by the [corporation](#) on the basis of [election](#) under section 897(i), unless there is attached to the [certification](#) a copy of the acknowledgment by the Internal Revenue Service of the [corporation's](#) [election](#), as required by [paragraph \(b\)\(2\)\(ii\)](#) of this section.

(iii) *Knowledge of falsity.* A [transferee](#) is not entitled to rely upon a transferor's [certification](#) if prior to or at the time of the [transfer](#) the [transferee](#) either—

(A) Has actual knowledge that the transferor's [certification](#) is false; or

(B) Receives a [notice](#) that the [certification](#) is false from a transferor's or [transferee's](#) agent, pursuant to § 1.1445–4.

(iv) *Belated notice of false certification.* If after the date of the [transfer](#) a [transferee](#) receives a [notice](#) that a [certification](#) is false, then that [transferee](#) is entitled to rely upon the [certification](#) only with respect to consideration that was paid prior to [receipt](#) for the [notice](#). Such a [transferee](#) is required to withhold a full 15 percent of the [amount](#) realized from the consideration that remains to be paid to the transferor if possible. Thus, if 15 percent or more of the [amount](#) realized remains to be paid to the transferor then the [transferee](#) is required to withhold and pay over the full 15 percent. The [transferee](#) must do so by [withholding](#) and paying over the entire [amount](#) of each successive [payment](#) of consideration to the transferor until the full 15 percent of the [amount](#) realized has been withheld and paid over. [Amounts](#) so withheld must be reported and paid over by the 20th day following the date on which each such [payment](#) of consideration is made. A [transferee](#) that is subject to the rules of this paragraph (b)(4)(iv) may not obtain a [withholding certificate](#) pursuant to § 1.1445–3, but must instead withhold and pay over the [amounts](#) required by this paragraph. For [dispositions](#) described in § 1.1445–1(b)(2), this paragraph shall be applied by replacing “15 percent” with “10 percent” each time it appears.

26 CFR § 1.6045-4 - Information reporting on real estate transactions with dates of closing on or after January 1, 1991.

§ 1.6045-4 Information reporting on real estate transactions with dates of closing on or after January 1, 1991.

(j) *Time and place for filing.* A reporting person shall file the information returns required by this section with respect to a real estate transaction after December 31 of the calendar year that includes the date of closing (as determined under paragraph (h)(2)(ii) of this section) and on or before February 28 (March 31 if filed electronically) of the following calendar year.

The returns shall be filed with the appropriate Internal Revenue Service Center at the address listed in the Instructions to Form 1099.

(k) [Reserved]

(l) *Requesting taxpayer identification numbers (TINS)*—(1) *Solicitation*—(i) *General requirements.* A reporting person who is required to make an information return with respect to a real estate transaction under this section must solicit a TIN from the transferor at or before the time of closing. The solicitation may be made in person or in a mailing that includes other items. Any person whose TIN is solicited under this paragraph (l) must furnish such TIN to the reporting person and certify that the TIN is correct. See paragraph (f)(2) of this section for rules that treat a husband and wife as a single transferor (and provide for the TIN solicitation of either) in the absence of an allocation of gross proceeds under paragraph (i)(5) of this section.

(ii) *Content of solicitation.* The solicitation shall be made by providing to the person from whom the TIN is solicited a written statement that the person is required by law to furnish a correct TIN to the reporting person, and that the person may be subject to civil or criminal penalties for failing to furnish a correct TIN. For example, the solicitation may be worded as follows:

You are required by law to provide [insert name of reporting person] with your correct taxpayer identification number. If you do not provide [insert name of reporting person] with your correct taxpayer identification number, you may be subject to civil or criminal penalties imposed by law.

The solicitation shall contain space for the name, address, and TIN of the person from whom the TIN is solicited and for the person to certify under penalties of perjury that the TIN furnished is that person's correct TIN. The wording of the certification must be substantially similar to the following: “Under penalties of perjury, I certify that the number shown on this statement is my correct taxpayer identification number.” The requirements of this paragraph (l)(1)(ii) may be met by providing to the transferor a copy of Form W-9. In the case of a real estate transaction for which a Uniform Settlement Statement is used, the requirements of this paragraph (l)(1)(ii) may be met by providing to the transferor a copy of such statement that is modified to conform to the requirements of this paragraph (l)(1)(ii).

(iii) *Retention requirement.* The solicitation shall be retained by the reporting person for four years following the close of the calendar year that includes the date of closing (as determined under paragraph (h)(2)(ii) of this section). Such solicitation must be made available for inspection upon request by the Internal Revenue Service.

SAMPLE FILE CLOSING CHECKLIST

Insured: _____ File #: _____

Closer: _____ Date: _____

ACTION	INITIALS	DATE
1. Change master file register from active to closed status and enter date and closed file number in closed file register.		
2. Confirm file ledger card reflects zero balance.		
3. Confirm all original documents filed or recorded.		
4. Confirm all third party property delivered (e.g. deeds, mortgages, policies, closing packages).		
5. Copy commitment, policies and examiner notes and file		
6. Review file for documents to be included in forms system.		
7. Duplicate documents, unused note pads, etc., removed from file (DO NOT remove draft work product, memos, phone messages, research notes, etc.).		
8. Check for loose, unfiled documents and place in the file.		
9. If an unsatisfied judgment is involved, diary the file for 3, 6, and 9 years to review assets and renewal of judgment prior to the expiration of 10 years.		
10. If UCC is involved, diary the file for renewal of UCC filing.		
11. If the file involves a lease or option to buy, diary the file for 6 months prior to expiration.		
12. If the file involves a criminal matter, check to see if expungement is possible and diary the file for 3 years.		
13. Final review by lawyer for any further work to be done and closing letter to client with return of any original documents.		
14. Assign destruction date and enter into calendar system and/or mark in closed file register or on index card.		

452 So.2d 1140

District Court of Appeal of Florida,
Fifth District.DOWDA AND FIELDS, P.A.,
and Alan B. Fields, Jr., Appellants,
v.
Donald R. COBB, Appellee.

No. 83-827.

|
July 19, 1984.**Synopsis**

In a successful action brought on a promissory note, judgment creditor's trial attorneys filed a notice of intent to claim a charging lien, and judgment creditor moved the court to dismiss the lien. The Circuit Court, Putnam County, Richard G. Weinberg, J., ordered trial attorneys to deliver their office files to successor counsel, and trial attorneys appealed. The District Court of Appeal, Cowart, J., held that: (1) trial attorneys did not have to deliver their office files to successor counsel who was retained by judgment creditor to defend judgment debtor's appeal from the judgment on the promissory note, and (2) after notice and opportunity to judgment creditor to be heard, trial court, on remand, was to hear and consider trial attorneys' motion to adjudicate a charging lien.

Reversed and remanded with directions.

West Headnotes (11)

- [1] **Attorneys and Legal Services** 🔑 Funds or property in attorney's possession in general
Attorneys and Legal Services 🔑 Judgment, settlement, or other recovery
Attorneys and Legal Services 🔑 Files, papers, and securities
 Attorney has possessory retaining lien on his client's papers, money, securities, and other property in his possession and, according to the circumstances, a charging lien on a judgment, award, or decree secured by him, or other

property recovered, for his client for fees and costs due him for services rendered to the client in recovering such judgment or property.

2 Cases that cite this headnote

- [2] **Attorneys and Legal Services** 🔑 Special or charging lien

Attorney's charging lien is not dependent upon possession but is based on equitable principles; client should not be allowed to appropriate the whole of a judgment, award, or decree if attorney who has secured it has not been compensated.

2 Cases that cite this headnote

- [3] **Attorneys and Legal Services** 🔑 Operation and effect of replacement or substitution

Office file maintained by attorney, relating to matters involving professional services performed for a particular client as to a particular matter, is the personal property of the attorney.

5 Cases that cite this headnote

- [4] **Attorneys and Legal Services** 🔑 Operation and effect of replacement or substitution

Office file maintained by attorney, relating to matters involving professional services performed for a particular client as to a particular matter, may contain information about a client's affairs concerning which attorney may have an ethical duty to communicate to a successor counsel.

4 Cases that cite this headnote

- [5] **Commercial Paper** 🔑 Attorney fees and costs

Contractual provision of promissory note for payment of attorney fees was for indemnification of client, who was the contracting party to the note, so that judgment on the note in favor of client awarded sums for attorney fees to client, as judgment creditor, and not to client's attorneys.

[6] Appeal and Error 🔑 Parties to whom security to be given

Supersedeas bond filed by judgment debtors for their appeal from a judgment on a promissory note provided security for judgment creditor but not for judgment creditor's attorneys.

[7] Attorneys and Legal Services 🔑 Notice

Mere filing by judgment creditor's attorneys of a notice of intent to claim a charging lien in the pending original action on promissory note did not establish charging lien against the judgment on the note nor give adequate constructive notice of the charging lien to parties dealing with judgment creditor with respect to the judgment.

[3 Cases that cite this headnote](#)

[8] Attorneys and Legal Services 🔑 Nature and form of proceeding

Though there may be other proper remedies for enforcement of an attorney's charging lien, such lien is commonly enforced against the judgment by summary proceedings in the original action.

[2 Cases that cite this headnote](#)

[9] Attorneys and Legal Services 🔑 Operation and effect of replacement or substitution

Judgment creditor's trial attorneys did not have to deliver their office files to successor counsel, who was retained by judgment creditor to defend judgment debtor's appeal from judgment in favor of judgment creditor on a promissory note, where there was no evidence or other indication that office files contained property of judgment creditor, and no reason was given as to why office files were needed by judgment creditor or successor counsel in order to defend judgment debtor's appeal.

[2 Cases that cite this headnote](#)

[10] Appeal and Error 🔑 Costs and fees

After notice and opportunity to client to be heard, trial court, on remand, was to hear and consider

motion of client's trial attorneys to adjudicate a charging lien and, if an indebtedness for legal services was found to be due trial attorneys from client and if that indebtedness was secured by a charging lien against final judgment rendered in favor of client in underlying action, then trial court was to adjudicate the indebtedness and lien and impress the judgment with that lien, instructing clerk of court to make marginal notation on recorded judgment so as to give constructive notice of trial attorneys' charging lien against the judgment.

[1 Cases that cite this headnote](#)

[11] Attorneys and Legal Services 🔑 Effect of contracts

In order for an attorney's charging lien to be imposed, there must first be a contract, express or implied, between the attorney and client.

[1 Cases that cite this headnote](#)

Attorneys and Law Firms

***1141** Alan B. Fields, Jr. of Dowda & Fields, Palatka, for appellants.

Michael W. Jones of Baxley & Jones, Gainesville, for appellee.

Opinion

COWART, Judge.

This case involves an attorney's charging lien on a judgment obtained by him for his client.

Appellants, original attorneys for appellee, brought suit on a promissory note and recovered judgment in favor of appellee, as judgment creditor, and against certain ***1142** judgment debtors. When the judgment debtors filed a supersedeas bond and undertook to appeal, appellee discharged appellants as counsel and retained other counsel to represent appellee on that appeal. Appellants then filed in the original action a paper entitled Notice of Intent to Claim Charging Lien. Appellee moved the court to dismiss appellants' attorney's charging lien alleging that appellants were asserting a retaining lien

on appellee's file, that appellee needed "his file" to defend the judgment debtors' appeal and that appellants were not entitled to both an attorney's charging lien and attorney's retaining lien. Appellants denied the assertion of a retaining lien stating that it retained only its own office file which contained no papers or documents belonging to the appellee, all of which had been introduced as evidence in the original action. Appellants also moved the trial court to adjudicate and impress an attorney's charging lien against the judgment that appellants, as counsel, had recovered in favor of appellee. By order dated April 19, 1983, the trial court ordered appellants to deliver their entire office file (with the exception of intra-office notices and memoranda) to successor counsel finding that appellants were "fully secured by the final judgment, the supersedeas bond and the charging lien filed by him in this action." This is an appeal of the order of April 19, 1983.

[1] [2] In Florida, as in most states, an attorney has a possessory retaining lien¹ on his client's papers, money, securities and other property in his possession and, according to the circumstances, a charging lien on a judgment, award or decree secured by him, or other property recovered, for his client² for fees and costs due him for services rendered to the client in recovering such judgment or property. The charging lien is not dependent upon possession, but is based on equitable principles; the client should not be allowed to appropriate the whole of a judgment, award or decree if the attorney who has secured it has not been compensated.

[3] [4] Attorneys normally maintain an office file relating to matters involving professional services performed for a particular client as to a particular matter. This is commonly referred to as that client's file but it only relates to that client and the file and its contents is the personal property of the attorney. The attorney's file may or may not contain documents or other property of the client. The attorney's file may also contain information about a client's affairs concerning which the attorney may have an ethical duty to communicate to successor counsel. There is no evidence or other indication that the attorney's file in this case contained property of the client. The client's promissory note had been reduced to final judgment and the litigation is over except for the appeal. No reason has been offered why appellants' office

file is needed by the client or successor counsel in order to defend the appeal, nor can we imagine one.

*1143 [5] [6] [7] [8] [9] [10] [11] The promissory note contained a provision for payment of attorney's fees and the judgment included sums on that account. However, the contractual provision for attorney's fees is for indemnification of the contracting party and the judgment awards sums for attorney's fees to the client, as judgment creditor, and not to the creditor's attorneys. Likewise, the supersedeas bond provides security for the client, as judgment creditor, but not for appellants, the creditor's attorneys who recovered the judgment for the judgment creditor. The mere filing of a notice of intent to claim a charging lien in the pending original action by the attorney does not establish the attorney's lien against the judgment nor give adequate constructive notice of the attorney's charging lien to parties dealing with the client with respect to the judgment. Although there may be other proper remedies for enforcement³ of an attorney's lien, it is commonly enforced against the judgment by summary proceedings in the original action. We reverse the order directing appellants to deliver their office files to successor counsel and direct that, after notice and opportunity to the client to be heard, the trial court hear and consider appellants' motion to adjudicate a charging lien and, if an indebtedness for legal services is found to be due appellants from appellee⁴ and if that indebtedness is secured by an attorney's charging lien against the final judgment, then the trial court should adjudicate the indebtedness and lien, and impress the judgment with that lien, instructing the clerk of the court to make a marginal notation on the recorded judgment so as to give constructive notice of appellants' charging lien against the judgment.

REVERSED AND REMANDED WITH DIRECTIONS.

DAUKSCH, J., and COLEMAN, T.P., Associate Judge, concur.

All Citations

452 So.2d 1140

Footnotes

- ¹ See generally *Chancey v. Bauer*, 97 F.2d 293 (5th Cir.1938); *Cooper v. McNair*, 49 F.2d 778 (D.C.Fla.1931); *Gray v. Hopkins-Carter Hardware Co.*, 32 F.2d 876 (5th Cir.1929); *Wilkerson v. Olcott*, 212 So.2d 119 (Fla. 4th DCA 1968); 7A

C.J.S., Attorney and Client, § 358 (1980); Annot., Rights and Remedies of Client as Regards Papers and Documents On Which Attorney Has Retaining Lien, 3 A.L.R.2d 148 (1949).

- 2 See generally *United States v. Transocean Airlines, Inc.*, 356 F.2d 702 (5th Cir.1966); *Sinclair, etc., and Zavertrnik, P.A. v. Baucom*, 428 So.2d 1383 (Fla.1983); *Winn v. City of Cocoa*, 75 So.2d 909 (Fla.1954); *Nichols v. Kroelinger*, 46 So.2d 722 (Fla.1950); *Greenfield Villages v. Thompson*, 44 So.2d 679 (Fla.1950); *In Re Warner's Estate*, 160 Fla. 460, 35 So.2d 296 (1948); *Miller v. Scobie*, 152 Fla. 328, 11 So.2d 892 (1943); *Scott v. Kirtley*, 113 Fla. 637, 152 So. 721, 93 A.L.R. 661 (1933); *Alyea v. Hampton*, 112 Fla. 61, 150 So. 242 (1933); *Pasin v. Kroo*, 412 So.2d 43 (Fla. 3d DCA 1982); *Miles v. Katz*, 405 So.2d 750 (Fla. 4th DCA 1981); *Conroy v. Conroy*, 392 So.2d 934 (Fla. 2d DCA 1980); *de la Cruz v. Brown*, 338 So.2d 245 (Fla. 3d DCA 1976); *Billingham v. Thiele*, 107 So.2d 238 (Fla. 2d DCA 1958); 7A C.J.S., Attorney and Client § 359 (1980); Annot., Attorney's Lien on Property Recovered For His Client, 93 A.L.R. 667, 696 (1934); 4 Fla.Jur.2d, Attorneys at Law § 158 (1978); Note, *Attorney and Client: Attorney's Charging Lien*, 4 U.Fla.L.Rev. 58 (1951); 10 Williston on Contracts § 1285B (3d ed. 1967).
- 3 See Annot., Attorney's Lien on Property Recovered—Remedies for Enforcement, 93 A.L.R. 667, 696 (1934).
- 4 In order for a charging lien to be imposed, there must first be a contract, express or implied, between the attorney and client. *Greenfield Villages, Inc. v. Thompson*, 44 So.2d 679 (Fla.1950); *Scott v. Kirtley*, 113 Fla. 637, 152 So. 721 (1933); *Alyea v. Hampton*, 112 Fla. 61, 150 So. 242 (1933).

End of Document

© 2022 Thomson Reuters. No claim to original U.S. Government Works.

FLORIDA BAR ETHICS OPINION
OPINION 81-8
January 16, 1981

Advisory ethics opinions are not binding.

A lawyer who intends to dispose of clients' files should make a diligent attempt to contact all clients and determine their wishes concerning their files. The file of any client who cannot be located must be reviewed individually and may be destroyed only after it is determined that no important papers of the client are in the file. A lawyer who is closing his practice should place files containing important papers in storage or turn them over to the attorney who assumes control of his active files.

CPR: EC 4-6
Opinions: 63-3, 71-62

Vice Chairman Mead stated the opinion of the committee:

This is an unusual inquiry from a young lawyer who has been diagnosed as having terminal cancer and who, in view of his limited life span, has requested advice as to the disposition of his client files. Specifically, the attorney asks if, after sending a letter to his clients advising them of his proposed course of action, he can destroy the files of those clients who do not respond (or who express no desire to retrieve their files) after a period of 90 days.

In disposing of clients' files, for whatever reason, the attorney must place primary emphasis on the desires of the client. The only provision of the Code of Professional Responsibility dealing specifically with the subject of the maintenance of client files is EC 4-6, which states in part:

A lawyer should also provide for the protection of the confidences and secrets of his client following the termination of the practice of the lawyer, whether termination is due to death, disability or retirement. For example, a lawyer might provide for the personal papers of the client to be returned to him and for the papers of the lawyer to be delivered to another lawyer or to be destroyed. In determining the method of disposition, the instructions and wishes of the client should be a dominant consideration.

It is incumbent upon the attorney to make an attempt to contact all clients whose files are in his possession. As this Committee stated in Opinion 71-62, "written inquiry should be sent requesting clients' advice as to their wishes in disposing of their files." This communication can be made by sending a letter to each clients' last known address or, if there is no address available, by publication in the local newspaper, requesting the client either to pick up his files or to give permission for their destruction.

This Committee has never attempted to delineate the specific period of time that a client's file must be kept by a lawyer; indeed, it is the contents of the file, not its date, that should dictate the length of time a file is to be retained. There may be some original documents in the file that

are vital to a client's interests and which must be preserved regardless of when they were prepared or executed. We adhere to the statement of this Committee in Opinion 63-3 that "Where the client is not available, we believe it desirable to check the file for certainty that no important papers are being disposed of before destroying them."

After a diligent attempt to contact all clients whose files are subject to destruction, the attorney should then dispose of all files in accordance with his clients' directives. The problem, of course, arises in connection with those clients who cannot be reached. We have a deep feeling for the inquiring attorney's situation and we appreciate his desire to proceed in accordance with the guidelines established in the Code; however, it is our opinion that client files cannot be automatically destroyed after 90 days, but that the files of those clients who do not respond must be reviewed individually by the attorney and can be destroyed by him only after he is satisfied that no important papers of the clients are contained in the file. If the attorney does find any such papers, he should have them indexed and either placed in storage or turned over to any attorney who assumes control of his active files.

Obviously, this is the first inquiry of this nature to be considered by the Committee, and we are not attempting to set forth hard and fast rules in making our determination. However, we note that the inquiring attorney has been in practice only slightly more than seven years and his closed files are not so old as to obviate the need for review.

FLORIDA BAR ETHICS OPINION
OPINION 63-3
June 25, 1963

Advisory ethics opinions are not binding.

The length of time a lawyer's files should be maintained depends largely on the importance of a file's contents. If the client is available, he should be requested to pick up the contents or authorize the attorney to dispose of the material. There is no obligation to invest funds of clients who cannot be located, but they should be deposited in a trust account where they would be insured and draw interest. When a settlement was effectuated on behalf of a wife, and both husband and wife executed the release, it is doubtful that it would be proper to issue a check to the wife alone.

Note: See Rule 5-1.1(f) regarding "Unidentifiable Trust Fund Accumulations and Trust Funds Held for Missing Owners."

Canons: 11, 37

Chairman Holcomb stated the opinion of the committee:

The Professional Ethics Committee has considered the matters presented by a member of The Florida Bar relative to disposal of old files and other matters.

With regard to the disposal of files, we believe that the length of time a file should be maintained depends largely on the contents of the file itself. However, if it is desired to dispose of a file, we believe that the client should be notified and asked to pick up the material or give authority to dispose of it in case there is any question. Where the client is not available, we believe it desirable to check the file for certainty that no important papers are being disposed of before destroying them.

As to funds held on behalf of a client who cannot be located, we find no obligation to invest the funds, but believe it would be advisable to deposit the same in a trust account in the name of the client, with the lawyer as trustee, with some bank or savings and loan association where the funds would be insured and would draw interest.

With regard to the third question, we are somewhat in doubt as to the propriety of issuing a check solely to the wife because, if the husband had some interest in the funds, he might thereby be precluded.

FLORIDA BAR ETHICS OPINION
OPINION 71-62
January 25, 1972

Advisory ethics opinions are not binding.

In disposing of clients' files the dominant consideration should be the instructions and wishes of the clients. Written inquiry should be sent requesting the clients' advice as to their wishes in disposing of their files.

CPR: EC 4-6

Chairman Clarkson stated the opinion of the committee:

A member of The Florida Bar seeks our advice concerning procedures to be followed upon change in the membership of a professional association. His letter of inquiry details the following factual background:

The firm was comprised of six members, two associates and an affiliated counsel. One of the members announced his withdrawal and acceptance of a position with another law firm. A second member thereupon indicated an intention to withdraw in order to practice as a sole practitioner. Several days later two more members announced their decision to withdraw from the firm intending to practice together. Several days after the latter decision was announced, the four members agreed to create their own law firm upon withdrawal.

The four withdrawing members owned 52 percent of the outstanding stock of the professional association under which organization the attorneys practiced law. The remaining members of the firm own the remaining 48 percent.

As a result of negotiations between the withdrawing and remaining partners, the following matters were agreed upon:

1. The withdrawing members took with them, after signing receipts therefor, a number of client files, both open files on which they were working and closed files that they had worked on.
2. A number of other files were to stay with the firm until a letter was produced signed by the client directing the firm to turn over the files to the withdrawing members.
3. Original wills for clients whose files were taken by the withdrawing members were also taken by them after signing receipts therefor. These wills have been held by the firm in safety deposit boxes owned by the firm, such custody at clients' direction.

4. It was agreed that mail directed to a withdrawing member at the firm address would be opened by the firm unless marked personal and that on matters relating to files taken by the withdrawing members, mail would be delivered to the withdrawing members.

5. The firm established a policy for answering telephone calls to the firm where the calling party requests to speak to one of the withdrawn members. Such policy was to advise the caller that the member had withdrawn from the firm, inquire of the caller as to whether he would like to speak to a remaining member. The telephone number of the withdrawing member was given upon request of the caller. Any remaining member who speaks with the caller would also furnish the number for the withdrawn partner.

The opinion of your committee is requested as to the propriety of each of the foregoing procedures, the first four of which were agreed upon by remaining and withdrawing members, while the fifth was not.

We perceive some conceptual difficulty in treating this inquiry as a routine withdrawal by one or more members of a law firm because (1) the law practice is carried on by a corporation and (2) it appears that most of the members are “withdrawing” rather than “remaining.” We must assume that it is the corporation which will continue to practice at the same location with such name change as may be appropriate.

The Committee has concluded that the procedures as outlined, particularly paragraphs 1 and 3, should be supplemented to afford existing clients an opportunity to direct disposition of their files or other legal papers. In determining the method of disposition, the instructions and wishes of the client should be a dominant consideration. EC 4-6, CPR. Ideally, this can best be accomplished by a written notice to these clients advising of the change in the membership of the professional association and requesting the clients’ advice as to their wishes in disposing of their files.

Subject to the foregoing comments, the Committee finds nothing objectionable in the proposal set forth above.

FLORIDA BAR ETHICS OPINION
OPINION 10-2
September 24, 2010

Advisory ethics opinions are not binding.

A lawyer who chooses to use Devices that contain Storage Media such as printers, copiers, scanners, and facsimile machines must take reasonable steps to ensure that client confidentiality is maintained and that the Device is sanitized before disposition, including: (1) identification of the potential threat to confidentiality along with the development and implementation of policies to address the potential threat to confidentiality; (2) inventory of the Devices that contain Hard Drives or other Storage Media; (3) supervision of nonlawyers to obtain adequate assurances that confidentiality will be maintained; and (4) responsibility for sanitization of the Device by requiring meaningful assurances from the vendor at the intake of the Device and confirmation or certification of the sanitization at the disposition of the Device.

RPC: 4-1.1, 4-1.6(a), 4-5.3(b)

The Professional Ethics Committee has been asked by the Florida Bar Board of Governors to write an opinion addressing the ethical obligations of lawyers regarding information stored on hard drives. An increasing number of devices such as computers, printers, copiers, scanners, cellular phones, personal digital assistants (“PDA’s”), flash drives, memory sticks, facsimile machines and other electronic or digital devices (collectively, “Devices”) now contain hard drives or other data storage media¹ (collectively “Hard Drives” or “Storage Media”) that can store information.² Because many lawyers use these Devices to assist in the practice of law and in doing so intentionally and unintentionally store their clients’ information on these Devices, it is important for lawyers to recognize that the ability of the Devices to store information may present potential ethical problems for lawyers.

For example, when a lawyer copies a document using a photocopier that contains a hard drive, the document is converted into a file that is stored on the copier’s hard

¹ As used in this opinion, Storage Media is any media that stores digital representations of documents.

² See Brian Smithson, *The IEEE 2600 Series: An Introduction to New Security Standards for Hardcopy Devices*, ISSA JOURNAL, Nov. 2009, at 28; Holly Herman, *Experts Warn Copiers Can Be Fertile Ground for ID Thieves*, READING EAGLE (Jun. 2, 2010, 12:28:54 P.M.), <http://readingeagle.com/article.aspx?id=222523>; Mark Huffman, *Digital Copiers Could Be an Identity Theft Threat*, ConsumerAffairs.com (May 19, 2010), http://www.consumeraffairs.com/news04/2010/05/digital_copiers.html; Armen Keteyian, *Digital Photocopiers Loaded with Secrets*, CBSNews.com (April 15, 2010), <http://www.cbsnews.com/stories/2010/04/19/eveningnews/main6412439.shtml>; Gregg Kelzer, *Photocopiers: The Newest ID Theft Threat*, COMPUTERWORLD (March 14, 2007), http://www.computerworld.com/s/article/9013104/Photocopiers_The_newest_ID_theft_threat.

drive. This document usually remains on the hard drive until it is overwritten or deleted. The lawyer may choose to later sell the photocopier or return it to a leasing company. Disposal of the device without first removing the information can result in the inadvertent disclosure of confidential information.

Duty of Confidentiality

Lawyers have an ethical obligation to protect information relating to the representation of a client. Rule 4-1.6(a) of the Rules Regulating the Florida Bar addresses the duty of confidentiality and states:

(a) Consent Required to Reveal Information. A lawyer shall not reveal information relating to representation of a client except as stated in subdivisions (b), (c), and (d), unless the client gives informed consent.

The comment to the rule further states:

The confidentiality rule applies not merely to matters communicated in confidence by the client but also to all information relating to the representation, whatever its source. A lawyer may not disclose such information except as authorized or required by the Rules of Professional Conduct or by law.

A lawyer must ensure confidentiality by taking reasonable steps to protect all confidential information under the lawyer's control. Those reasonable steps include identifying areas where confidential information could be potentially exposed. Rule 4-1.1 addresses a lawyer's duty of competence:

Competence A lawyer shall provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness, and preparation reasonably necessary for the representation.

The comment to the rule further elaborates:

To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law *and its practice*, engage in continuing study and education, and comply with all continuing legal education requirements to which the lawyer is subject.

(emphasis added).

If a lawyer chooses to use these Devices that contain Storage Media, the lawyer has a duty to keep abreast of changes in technology to the extent that the lawyer can identify potential threats to maintaining confidentiality. The lawyer must learn such details as whether the Device has the ability to store confidential information, whether the information can be accessed by unauthorized parties, and who can potentially have access to the information. The lawyer must also be aware of different environments in which confidential information is exposed such as public copy centers, hotel business centers,

and home offices. The lawyer should obtain enough information to know when to seek protection and what Devices must be sanitized, or cleared of all confidential information, before disposal or other disposition. Therefore, the duty of competence extends from the receipt, i.e., when the lawyer obtains control of the Device, through the Device's life cycle, and until disposition of the Device, including after it leaves the control of the lawyer. Further, while legal matters are beyond the scope of an ethics opinion, a lawyer should be aware that depending on the nature of the information, misuse of these Devices could result in inadvertent violation of state and federal statutes governing the disclosure of sensitive personal information such as medical records, social security numbers, criminal arrest records, etc.

Duty to Supervise

The lawyer must regulate not only the lawyer's own conduct but must take reasonable steps to ensure that all nonlawyers over whom the lawyer has supervisory responsibility adhere to the duty of confidentiality as well. Rule 4-5.3(b) states:

(b) Supervisory Responsibility. With respect to a nonlawyer employed or retained by or associated with a lawyer or an authorized business entity as defined elsewhere in these Rules Regulating The Florida Bar:

(1) a partner, and a lawyer who individually or together with other lawyers possesses comparable managerial authority in a law firm, shall make reasonable efforts to ensure that the firm has in effect measures giving reasonable assurance that the person's conduct is compatible with the professional obligations of the lawyer;

(2) a lawyer having direct supervisory authority over the nonlawyer shall make reasonable efforts to ensure that the person's conduct is compatible with the professional obligations of the lawyer; and

(3) a lawyer shall be responsible for conduct of such a person that would be a violation of the Rules of Professional Conduct if engaged in by a lawyer if:

(A) the lawyer orders or, with the knowledge of the specific conduct, ratifies the conduct involved; or

(B) the lawyer is a partner or has comparable managerial authority in the law firm in which the person is employed, or has direct supervisory authority over the person, and knows of the conduct at a time when its consequences can be avoided or mitigated but fails to take reasonable remedial action.

A lawyer's supervisory responsibility extends not only to the lawyer's own employees but over entities outside the lawyer's firm with whom the lawyer contracts to assist in the care and maintenance of the Devices in the lawyer's control. If a nonlawyer

will have access to confidential information, the lawyer must obtain adequate assurances from the nonlawyer that confidentiality of the information will be maintained.

Sanitization

A lawyer has a duty to obtain adequate assurances that the Device has been stripped of all confidential information before disposition of the Device. If a vendor or other service provider is involved in the sanitization of the Device, such as at the termination of a lease agreement or upon sale of the Device, it is not sufficient to merely obtain an agreement that the vendor will sanitize the Device upon sale or turn back of the Device. The lawyer has an affirmative obligation to ascertain that the sanitization has been accomplished, whether by some type of meaningful confirmation, by having the sanitization occur at the lawyer's office, or by other similar means.

Further, a lawyer should use care when using Devices in public places such as at copy centers, hotel business centers, and outside offices where the lawyer and those under the lawyer's supervision have little or no control. In such situations, the lawyer should inquire and determine whether use of such Devices would preserve confidentiality under these rules.

In conclusion, when a lawyer chooses to use Devices that contain Storage Media, the lawyer must take reasonable steps to ensure that client confidentiality is maintained and that the Device is sanitized before disposition. These reasonable steps include: (1) identification of the potential threat to confidentiality along with the development and implementation of policies to address the potential threat to confidentiality; (2) inventory of the Devices that contain Hard Drives or other Storage Media; (3) supervision of nonlawyers to obtain adequate assurances that confidentiality will be maintained; and (4) responsibility for sanitization of the Device by requiring meaningful assurances from the vendor at the intake of the Device and confirmation or certification of the sanitization at the disposition of the Device.

Policies and Procedures
Privacy and Information Security

Purpose	Document a privacy and information security program (policies and procedures) to help ensure (insert name of entity /agency) maintains written protocols for the protection of data and Non-public Personal Information (NPI).
Scope	These policies and procedures are for all of (insert name of entity /agency) (hereafter referred to as “The Company”) locations including all satellite offices. These procedures are to be followed by all employees and independent contractors where applicable.
Procedures	<p><i>[The Company should review its legal, contractual, and statutory requirements for privacy and information security and incorporate those requirements in these procedures.]</i></p> <p>The Company has a formal privacy and information security program that is appropriate with the size and complexity, the nature and scope of the Company’s activities and the sensitivity of the information in the Company’s possession. As part of this program, The Company maintains a Privacy Policy Notice (see attached) that is posted on The Company’s website and provided to customers and consumers for each order processed. Additional information about The Company’s privacy and information security program is available to consumers and customers upon request.</p> <p>The Company policies associated with the privacy and information security program are given to all employees and the employees must acknowledge in writing that they have read and understand such policies. It is the responsibility of (insert role/function) to help ensure The Company has received all employee acknowledgements.</p> <p>The Company makes an assessment (insert frequency) of the standards and requirements affiliated with The Company’s information security program, including those set out in this policy and procedure document. This assessment is conducted by (insert role/function/vendor) and a formal report on compliance is issued to The Company management.</p> <p>Physical Security of NPI</p> <p>The Company utilizes (insert vendor name) as the information provider for background and credit checks. The Company individuals who have access to NPI is restricted to authorized principals and employees who have undergone a formal background check and credit report process which identified no irregularities.</p> <p>Removable media devices, including but not limited to external hard drives, compact discs, magnetic tapes and USB/flash drives are issued by the Company with the approval of (insert role/function). The use of removable</p>

media devices is prohibited unless **(insert role/function)** has authorized such use. Removable media is kept in a secure area and accounted for via **(insert method or role/function)** when not in use.

Other standard procedures for security of NPI include closing paper files other than the one currently being worked on, stow files away when away from workspace and lock desks and file cabinets at the end of the day. Hardcopy NPI that is transmitted outside The Company is done so using only secured envelopes and/or locked document bags.

Network Security of NPI

At the direction of **(insert role/function)**, The Company's designated Network Administrator grants appropriate access to The Company's various computer technology applications. The Company's file server(s) or main central processing unit is housed **(describe where and if in a secured environment)**. The Company's computer network utilizes up-to-date anti-virus, anti-spyware and data encryption software applications. The Network Administrator is responsible for such software maintenance.

Access to The Company's information technology computers and network is secured by individual and unique passwords. The Company utilizes a computer application that prompts employees to change passwords in regular frequency **(specify frequency, i.e. 90/60/30 days)**. All The Company's computers no mater, desktop or laptop run a "screen timeout" application causing automatic system sign off when the system detects no activity for a period of **(insert length of time)**.

Disposal of NPI

The Company has defined and communicated to employees the types of data/information that falls into the NPI category. Any NPI data is disposed of accordingly. Paper records by shredding. Small shredders are available throughout the office. Large, secure shredding bins provided by **(insert vendor name)** can also be found in the office. When disposing of computers and portable storage devices, The Company uses a software application to erase/wipe clean the device.

Disaster Management Plan for NPI

The Company has a documented disaster management plan to help ensure adequate back-up, recovery and business continuation procedures. The plan also includes required procedures for notification and response to security incidents and breaches. **(Specify name of document, i.e. Disaster Management Plan)**. The Company also maintains insurance coverage **(Indicate types of insurance coverage including commercial property insurance, business interruption coverage, and cyber-security coverage if applicable)** for such circumstances. The disaster management plan is reviewed on an annual basis by **(insert role/function)** and updated as appropriate.

Security Practices of Independent Service Providers

If independent service providers for The Company receive NPI from The Company, The Company shares this policy document with the service provider and/or conducts appropriate due diligence of the NPI security measures of the service provider before transmitting any NPI data. Service providers are aware they must notify The Company regarding NPI security breaches of NPI data that has been transmitted.

	If security breaches occur, proper notification is provided to consumers and law enforcement in accordance with The Company's privacy and information security program and disaster management plan.
--	--

Contact Officer	<i>Provide the position title and name of person(s)</i>
Date Approved	<i>Day Month Year</i>
Date of Commencement	<i>Day Month Year</i>
Amendment Dates	<i>List the dates the policy has been amended (Day Month Year)</i>
Date for Next Review	<i>Month Year</i>
Related References and Links	<i>Internal Company Policies:</i> <ul style="list-style-type: none"> • <i>Reference any specific privacy and information security program policies and where they are kept.</i>

SAMPLE FILE RETENTION AND DESTRUCTION POLICY

Effective _____, this company implemented this file retention and destruction policy:

File Retention and Destruction Policy

Original documents and other property belonging to others are delivered or returned no later than the conclusion of the matter for which this company has been engaged. Copies of relevant materials which we create or receive will also be provided within that time frame. Our file on a matter is held in storage for a specific retention period. Prior to storage files are culled according to the Guidelines for Culling Files. At the end of the prescribed retention periods, files are summarily destroyed.

Guidelines for Destruction of Inactive Title Insurance Transaction Files

Purpose: Inactive title insurance transaction files may not be destroyed until the periods of time related to statutory, regulatory, contractual, and customer service guidelines have expired. This period of time ("retention period") commences on the date our work on a matter has been completed.

Procedure:

1. Files are archived until a regularly scheduled file destruction event arrives which is after a file's targeted destruction date.
2. The targeted destruction date is that date entered into the respective File Closing Checklist form or the date ten (10) years from the date of the conclusion of the matter, whichever period is longer, provided the respective File Closing Checklist indicates that the file has been sufficiently culled and is ready for destruction. The targeted destruction date will also have been entered upon the appropriate office calendars.
3. If the File Closing Checklist does not then indicate readiness, the file will be set aside and culled pursuant to the Guidelines for Culling Files and a new destruction date will be assigned.

Guidelines for Culling Files

Purpose: A stripped-down file contains only those materials needed for legitimate business purposes including statutory, regulatory, contractual, and customer service requirements. A culled file is ready for destruction at the end of its designated retention period with only a cursory review of its status as an appropriately culled file. As such, it may not then contain any property belonging to others.

Procedure:

1. Prepare a cover letter and mail any original documents, copies or other property which have not yet been delivered to the client, customer, consumer or other party entitled to the property. If the property is not capable of such delivery, mail a notice to the party advising them to make an appointment to come and pick up the property within sixty (60) days or that the property will be appropriately disposed. Include a statement of the office's file retention policy in the cover letter or notice. If any action is necessary under this procedure, schedule a new date for culling the file that is more than sixty (60) days from the date of the transmittal letter.

2. Remove the following and place in a secured on-site container designated for shredding:
 - a. Notes and other memoranda.
 - b. Copies of materials which are published or recorded in public records which can be easily located again if necessary. (e.g. examined public records)
 - c. Duplicates.
3. Make a copy of any title insurance Schedules A and B and a copy of the examiner's chain of title and notes and file with other examinations of this subdivision, condominium, co-op, or section.
4. Complete the File Closing Checklist form and confirm the date to be assigned for file destruction and enter it into the form.
5. Confirm the stacking order of the file top to bottom as follows:
 - a. File Closing Checklist form
 - b. Copy of file ledger card reflecting zero balance
 - c. Client, customer or consumer receipts and letters of transmittal for all papers, documents, reports and other property delivered to them
 - d. Title insurance policies and marked up commitment
 - e. Post-closing title search results
 - f. Copies of recorded documents
 - g. Examiner's take off sheet
 - h. Title search reports
 - i. Settlement statement
 - j. Copies of outgoing checks and wire transfer confirmations
 - k. Payoff letters, invoices, estoppel notices, and tax information
 - l. Copies of incoming checks and wire transfer confirmations
 - m. Copies of professional reports obtained in connection with transaction (e.g. survey, WDO, inspections)
 - n. Copy of executed lender closing package with transmittal letter on top
 - o. Contract
 - p. Acknowledgement of File Retention and Destruction Policy and Consent to File Destruction

Guidelines for Implementation of File Retention and Destruction Policy

Purpose: Implementation must involve providing notice to affected parties; acknowledgement of the policy by them and consent to its implementation; guidance to our employees to achieve consistency; and a readily accessible record of the actions which have taken place regarding a file.

Procedure:

1. Each newly opened file will include an *Acknowledgement of File Retention and Destruction Policy and Consent to File Destruction* form to be signed incident to the closing of the transaction. It will contain the following statement of policy:

“Original documents and other property belonging to you will be delivered to you no later than the conclusion of our work on this transaction at which time we will consider our file to be closed. Copies of relevant materials which we create, receive or are otherwise obligated to deliver will be provided to you within that time frame as well.

Any copy requests made by you after our file has been closed will be subject to the file’s availability and our charge for retrieving and copying the requested materials. Our files are kept for the specific retention period we assign to each based upon regulatory compliance and other factors. At the end of assigned retention periods, files are destroyed.”

2. Once all aspects of a transaction have been completed, our file will be culled in accordance with the procedure outlined in the Guidelines for Culling Files. The person culling the file will complete a File Closing Checklist form and include it as part of the closed file; make a notation in the office index for files that the file has been closed; and enter the date assigned for the file’s destruction into the office calendar.
3. At regularly scheduled intervals, all files which have reached the end of the assigned retention period since the last file destruction event will be summarily destroyed in accordance with the destruction procedures then in effect. At a minimum those procedures will include due precaution for the protection of Non-public Personal Information.

**Acknowledgement of File Retention and Destruction Policy
and
Consent to File Destruction**

In keeping with our commitment to keeping you informed, we are asking you to understand and acknowledge our responsibility as it relates to the continued maintenance of your file once this matter has concluded.

Please read the statement of policy below and sign where indicated to indicate your understanding of our file retention and destruction policy and your consent to its use as it relates to your transaction file.

POLICY

Original documents and other property belonging to you will be delivered to you no later than the conclusion of our work on this transaction at which time we will consider our file to be closed. Copies of relevant materials which we create, receive or are otherwise obligated to deliver will be provided to you within that time frame as well.

Any copy requests made by you after our file has been closed will be subject to the file's availability and our charge for retrieving and copying the requested materials. Our files are kept for the specific retention period we assign to each based upon regulatory compliance and other factors. At the end of assigned retention periods, files are destroyed.

PLEASE FEEL FREE TO ASK QUESTIONS BEFORE SIGNING THIS FORM.

I HEREBY ACKNOWLEDGE that I have read and understand the file retention and destruction policy adopted by this business and I CONSENT to the destruction of my transaction file in accordance with the policy.

(Name)

(Date)

CLOSED FILE ARCHIVE AND DESTRUCTION NOTICE

[Date]

[Addressee information]

Re:

Dear:

Our records indicate the above matter is concluded and I want to again thank you for the opportunity to have provided our services to you. I am writing to inform you that we are now in the process of moving the closed case file into archival storage. The file may include copies of records you want or need, such as documents we created for you. Please let us know within thirty (30) days of this letter's date whether you would like to obtain a copy of this file. The cost of copying will be billed to you at [xx] cents per page.

At the completion of the 30-day period, the file will be moved into off-site archival storage, and will then be subject to destruction according to the firm's record retention and destruction policy without further notice to you.

Thank you for your confidence in us.

Sincerely,

Sample Electronic File Policy

[Company]

Effective :[Date]

Last revised: [Date]

1. Electronic Files

All files that we create and maintain relating to client, customer or consumer matters, as well as this office's internal procedures, financial matters, and operations guides, are stored electronically. An electronic file is this company's actual office file related to that matter.

All incoming and outgoing paper documents are scanned daily and added to the respective electronic files. After scanning, paper documents are placed into a matter's paper file folder. Document Originals are handled as described below.

The paper file folders and their contents are shredded from time to time in accordance with this company's File Retention Policy.

2. Scanning

After review, all paper documents are placed into the secure sorting box designated for scanning. By the end of each day, the paper documents will have been scanned and uploaded to the office server into an electronic file designated as the general file relating to that matter. Once a paper document is scanned and uploaded to the office server, the electronic document shall become part of the actual office file. The paper file, and the papers it contains, is merely for convenience until the matter's final resolution.

3. File Backups

All electronic files are backed up daily by synchronizing the entire server to an external hard drive, which is then taken offsite. There are seven external hard drives that are backed up in rotation and kept offsite as follows:

- Daily A and Daily B [specify offsite location]
- Weekly A and Weekly B [specify offsite location]
- Monthly A and Monthly B [specify offsite location]
- Annual [specify offsite location]

In addition, whenever paper file folders are shredded, the electronic files are copied to three CDs and kept onsite and offsite at [specify locations] and are also copied to a remote online storage server by SSL-secured Internet transmission.

4. File Ownership

All files that we maintain belong to this company and not to the client, customer or consumer. The files and their contents constitute the personal property of the company. This includes both the electronic files and paper file folders. If a paper file folder contains Document Originals, those documents are handled as described below and are returned to the owner whenever possible.

5. Document Originals

Our policy is that we do not keep original documents that belong to others. If an original document is provided, we make a copy for our paper file folder, return the original to the client, and scan the copy as part of our standard scanning procedure. Therefore, the contents of our paper files do not contain any original documents. The only exceptions to this are as follows:

- Deeds, mortgages, satisfactions, releases, liens and other documents which we have undertaken responsibility for recording or delivery to others.
- If recorded either electronically or by physical delivery, the recorded Document Original is scanned to the file and then forwarded to the owner along with any other Document Originals in our possession (e.g. promissory notes).
- Original documents executed in connection with the settlement of a real estate transaction are distributed at settlement or held only as long as necessary and then mailed to the appropriate parties. Document Originals or duplicate Document Originals which are the property of this office are scanned as part of our standard scanning procedure.

6. Client Copies

In addition to the surrender of original documents as described above, our policy is to provide clients, customers and consumers with copies of all unprivileged documents related to the matter for which we have been engaged. These copies may be delivered in paper form or electronically. It is the client, customer or consumer's responsibility to secure, retain and otherwise accept stewardship of their original documents as well as the copies of documents that we provide.

7. Shredding Paper Files

Paper file shredding is performed either internally by an employee trained in the protection of Non-public Personal Information (NPI), or by a bonded outside service provider in such a manner that the provider cannot view contents of files. When performed by an outside provider, the paper is first stored in a secured on-site container and the subsequent shredding is observed by an employee of this office who has clearance to view NPI. Paper file folders which do not contain Document Originals owned by others can be shredded at any time as long as they have been scanned and uploaded to the office server.

You've Been Hacked – Now What? Responsibilities Under Florida's Information Protection Act and ALTA

By John St. Lawrence, Fund Legal Education Attorney

Sec. 501.171, F.S., also known as the Florida Information Protection Act of 2014 (FIPA) replaced Florida's "data breach notification law" in 2014. FIPA enacted significant new requirements for handling electronic data containing confidential personal information and giving customers notice in the event of a security breach. Given the recent sharp increase in fraudulent attempts to infiltrate e-mail communications surrounding real estate closings, Fund Members should become aware of their responsibilities in the event of an attack that may compromise customer information.

Who Is a "Covered Entity?"

Businesses and government entities that acquire, maintain, store, or use personal information are covered by FIPA. Third-party agents contracted to maintain, store, or process personal information on behalf of covered entities are also covered.

What Is "Personal Information?"

"Personal information" means either (a) a user name or e-mail address, in combination with a password or security question and answer that would permit access to an online account; or (b) an individual's first name or first initial and the individual's last name in combination with any of the following:

- A social security number;
- A driver's license or identification card number, passport number, military identification number, or other similar number issued on a government document used to verify identity;
- A financial account number or credit or debit card number, in combination with any required security code, access code, or password that is necessary to permit access to an individual's financial account;
- Any information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional; or
- An individual's health insurance policy number or subscriber identification number and any unique identifier used by a health insurer to identify the individual.

What Are Covered Entities' Responsibilities under FIPA?

Covered entities must take “reasonable measures” to protect and secure data containing personal information in electronic form, and must give notice to affected individuals and the Florida Department of Legal Affairs (FDLA) in the event of a significant breach.

What Is a “Breach of Security?”

“Breach of security” means unauthorized access to data containing personal information in electronic form. Good faith access by an employee or agent of the covered entity does not constitute a breach of security, so long as the information is not used for a purpose unrelated to the business, or subject to further unauthorized use.

When and How Must the Florida Department of Legal Affairs Be Notified of a Breach?

A covered entity must provide written notice to the FDLA of any breach affecting 500 or more individuals in Florida. The notice must be given “as expeditiously as practicable” and no later than 30 days after determination of the breach or reason to believe a breach occurred. Covered entities may receive an additional 15 days by providing good cause for the delay in writing within 30 days of the breach.

The written notice to the FDLA must include:

- A synopsis of events surrounding the breach;
- The number of individuals in Florida potentially affected;
- A note of any services offered free of charge to the affected individuals in connection with the breach;
- A copy of the notice sent to the affected individuals; and
- The name, address, phone number, and e-mail address of the employee or agent of the covered entity who can provide additional information about the breach.

In addition, upon request, the covered entity must provide:

- A police report, incident report, or computer forensics report;
- A copy of the policies in place regarding breaches; and
- Steps taken to rectify the breach.

What Notice Must be Given to Individuals?

Covered entities must notify each individual in Florida whose information was accessed, or the covered entity reasonably believes was accessed, due to the breach of security. Notice must be “expeditious” and “without unreasonable delay,” but no later than 30 days after the breach or reason to believe a breach occurred, unless the covered entity receives a waiver, or a delay is authorized under FIPA. No notice is required if, after investigation and consultation with law enforcement, the covered entity reasonably determines the breach has not and likely will not result in identity theft or other financial harm. This determination must be documented and provided to the FDLA within 30 days of the determination, and maintained for at least five years.

The notice to affected individuals must be made either in writing, sent to the mailing address in the records of the covered entity, or by e-mail to the e-mail address in the records of the covered entity.

The notice must contain, at a minimum:

- The date, estimated date, or estimated date range of the breach of security;
- A description of the personal information accessed or reasonably believed to have been accessed; and
- Information the individual can use to contact the covered entity to inquire about the breach and the personal information the covered entity maintained about the individual.

A covered entity may provide substitute notice by internet or broadcast media if the cost of providing notice would exceed \$250,000, because the number of affected individuals exceeds 500,000, or because the covered entity does not have an e-mail address or mailing address for the affected individuals. If a covered entity is required to give notice to more than 1,000 individuals at once, the covered entity must also notify all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined in the Fair Credit Reporting Act, of the timing, distribution, and content of the notices.

What Are the Requirements for Disposal of Customer Records?

Covered entities and third-party agents must take reasonable measures to dispose of customer records containing personal information within their custody or control when the records are no longer to be retained. Disposal must involve shredding, erasing, or otherwise modifying the personal information so as to make it indecipherable through any means.

What About a Breach of a System Maintained by a Third Party?

In the event of a breach of security of a system maintained by a third-party agent, such agent must notify the covered entity of the breach of security no later than 10 days following determination of the breach or reason to believe the breach occurred. Upon receiving notice from a third-party agent, a covered entity must provide the notices otherwise required.

How Does Enforcement Work?

A violation of FIPA is treated as an unfair or deceptive trade practice under Sec. 501.207, F.S. In addition, covered entities are liable for civil penalties of \$1,000 per day for the first 30 days after a violation and \$50,000 for each subsequent 30-day period, up to 180 days. If a violation continues for more than 180 days, additional fines may accrue, not to exceed \$500,000.

FIPA does not create a private cause of action.

Integration with Pillar 3 of ALTA's Best Practices

Pillar 3 of the American Land Title Association (ALTA) Best Practices paradigm calls for title agents to implement a written policy describing a plan to protect "non-public personal information" (NPI). See "ALTA Best Practice Pillar No. 3," 45 *Fund Concept* 110 (Oct. 2013).

ALTA's Best Practices call for compliance with applicable federal and local law, so FIPA compliance is inherently part of Pillar 3. Some Pillar 3 recommendations are met by compliance with FIPA, while others call for further action.

For example, FIPA compliance would cover the Pillar 3 recommendation calling for secure disposal of sensitive material by shredding or other means, which would also meet FIPA's requirement to render discarded information "indecipherable." Pillar 3's recommendation for notice to customers and law enforcement in the event of a breach "as required by law" similarly can be met by a policy conforming to FIPA requirements.

However, ALTA defines NPI more broadly than FIPA's "personal information," and calls for guarding more information, including:

- Any information that specifically recognizes an individual by unique descriptors;
- Information from customers on forms, applications, or information about a customer's transactions; or
- Information about a customer which is otherwise unavailable to the general public.

ALTA is more specific than FIPA as to the forms of security required to protect NPI, recommending a "clean desk policy" and background checks for employees who have access to NPI. Pillar 3 calls for title agents to control the use of removable media, and requires secure delivery methods for NPI.

Pillar 3 also goes beyond FIPA in calling for a disaster management plan to keep NPI secure in the event of emergency, and suggests carrying out drills to test the plan and to record the results of the drills.

Fund Members should be able to comply with both FIPA and ALTA's Best Practices Pillar 3 by preparing a written policy that meets all FIPA requirements, and adding specifics such as the background checks, physical security, and disaster plan contemplated by ALTA. Given the recent and continuous attempts by criminals to compromise e-mail accounts and perpetrate fraud in real estate transactions, there is no time like the present for Fund Members to make sure they are prepared to show compliance with FIPA and ALTA's Best Practices in the event of a security breach.

4/30/2017

CERTIFICATE OF ATTENDANCE

Certified Paralegals are required to record evidence of 50 hours of continuing legal education hours to renew the CP credential every 5 years. CLE hours are recorded in CPs' accounts through the [NALA online portal](https://www.nala.org/certification/certtest2view). Of the 50 hours, 5 hours must be in legal ethics, and no more than 10 hours may be recorded in non-substantive areas. If attending a non-NALA sponsored educational event, this certificate may be used to obtain verification of attendance. Please be sure to obtain the required signatures for verification of attendance. The requirements to maintain the CP credential are available from NALA's web site at <https://www.nala.org/certification/certtest2view>. Please keep this certificate in the event of a CLE audit or further information is needed.

PLEASE COMPLETE THE SPACES BELOW AND ATTACH A PROGRAM

Session Length In Hours	Session Topics (Description and Speakers)	Validation of Attendance
1.0	Record Retention & Disposal: Put It in Writing / Kara Scott	<i>Kara Scott</i>

Name of CP (Please Print)			NALA Account Number (On Mailing Label)		
			149113		
Signature of CP			Name of Seminar/Program Sponsor		
			Record Retention & Disposal: Put It in Writing / ATFS, LLC		
Address			Authorized Signature of Sponsor Representative		
			<i>Kara Scott</i>		
			Date of Educational Event:		
City:		State (XX):			
Preferred e-mail address			Location:		
			Recorded Webinar		

For Office Use Only	
Substantive hours	
Non-substantive hours	
Ethics	



The Florida Bar

651 East Jefferson Street
Tallahassee, FL 32399-2300

Joshua E. Doyle
Executive Director

850/561-5600
www.FLORIDABAR.org

Certificate of Accreditation for Continuing Legal Education

256131
Attorney's Title Fund Services
John St. Lawrence
PO Box 628600
Orlando, FL 32862-8600

Jan. 17, 2024

Reference Number: 2400634N

Title: Record Retention and Disposal: Put it in Writing

Level: Intermediate

Approval Period: 03/01/2024 - 09/30/2025

CLE Credits

General	1.0
Ethics	1.0

Certification Credits

Real Estate	1.0
-------------	-----