Protecting NPI – Pillar 3

Protecting Your Practice as You Protect Your Customers' NPI: An In-Depth Look at Best Practice Pillar 3 in 2 parts

LEGAL EDUCATION DEPARTMENT
Attorneys' Title Fund Services, Inc.

Please contact The Fund's Education Registrar
for information about our programs
EducationRegistrar@thefund.com
(888) 407-7775

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

Protecting NPI – Pillar 3

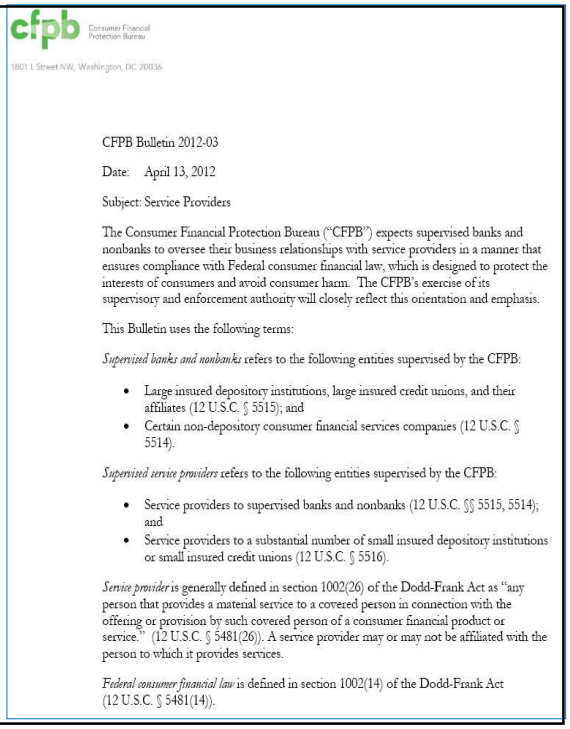
Protecting Your Practice as You Protect Your Customers' NPI: An In-Depth Look at Best Practice Pillar 3 – Part 1

Linda Monaco, B.C.S.
Senior Legal Education Attorney

3

Reaction to CFPB April 13, 2012 Bulletin

- Lender is responsible for the actions of all vendors
  - Settlement agent
- ALTA's Best Practices
  - Seven pillars



cfpb Consumer Financial Protection Bureau

1801 L Street NW, Washington, DC 20036

CFPB Bulletin 2012-03

Date: April 13, 2012

Subject: Service Providers

The Consumer Financial Protection Bureau ("CFPB") expects supervised banks and nonbanks to oversee their business relationships with service providers in a manner that ensures compliance with Federal consumer financial law, which is designed to protect the interests of consumers and avoid consumer harm. The CFPB's exercise of its supervisory and enforcement authority will closely reflect this orientation and emphasis.

This Bulletin uses the following terms:

Supervised banks and nonbanks refers to the following entities supervised by the CFPB:

- Large insured depository institutions, large insured credit unions, and their affiliates (12 U.S.C. § 5515); and
- Certain non-depository consumer financial services companies (12 U.S.C. § 5514).

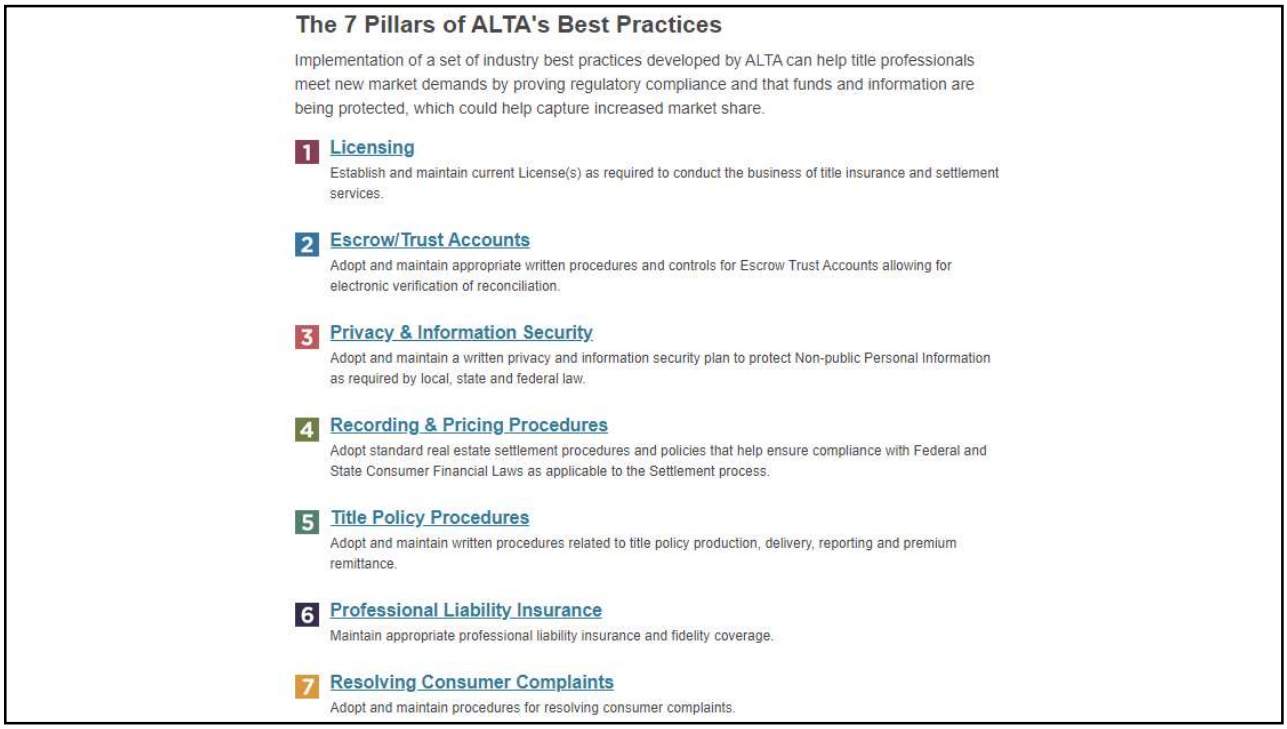
Supervised service providers refers to the following entities supervised by the CFPB:

- Service providers to supervised banks and nonbanks (12 U.S.C. §§ 5515, 5514); and
- Service providers to a substantial number of small insured depository institutions or small insured credit unions (12 U.S.C. § 5516).

Service provider is generally defined in section 1002(26) of the Dodd-Frank Act as "any person that provides a material service to a covered person in connection with the offering or provision by such covered person of a consumer financial product or service." (12 U.S.C. § 5481(26)). A service provider may or may not be affiliated with the person to which it provides services.

Federal consumer financial law is defined in section 1002(14) of the Dodd-Frank Act (12 U.S.C. § 5481(14)).

4



5

In-depth Considerations for Pillar 3 Protecting NPI

- 2014 rush to complete the Best Practices Manual
- 2015 new CD arrived
  - Lenders adjusted focus
- 2020 COVID-19
  - Push for electronic closings
  - Lenders still in paper mode
  - Increase request for Best Practice Manuals
- Now is time for an in-depth look at protecting NPI & Pillar 3

6

ALTA's Best Practices

Pillar 3

Adopt & maintain a written privacy & information security program to protect

Non-public Personal Information

as required by local, state, & federal law

7

Parts 1 & 2

- Part 1
  - NPI
  - Assessment
  - Audit & oversight
  - Documentation
  - Annual review
  - Third party requirements
  - Digital security
- Part 2
  - Data security
  - Physical security
  - Disaster preparedness
  - Employees & non-employees
  - Security breach notification

73*

*** ALTA Assessment Readiness Guide for Pillar 3**

The Fund

8

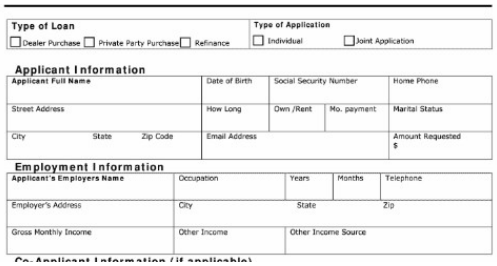
NPI

Non-public Personal Information

9

What is NPI?

- Generally – information not available to general public
  - Tax identification numbers
  - Birthdates
  - Employer
  - Mother's maiden name
- Location of NPI – digital or physical
  - Forms - intake
  - Applications
    - Employment



Type of Loan
☐ Dealer Purchase ☐ Private Party Purchase ☐ Refinance

Type of Application
☐ Individual ☐ Joint Application

Applicant Information

Applicant Full Name	Date of Birth	Social Security Number	Home Phone
Street Address	How Long	Own /Rent / Mo. payment	Marital Status
City State Zip Code	Email Address		Amount Requested $

Employment Information

Applicant's Employers Name	Occupation	Years / Months	Telephone
Employer's Address	City State Zip		
Gross Monthly Income	Other Income	Other Income Source	

10

Federal Law – 16 CFR Sec. 313.3 Definitions

94

- (n) Nonpublic personal information (NPI)
  - Directly identifiable information
  - Group of information (can be available to public) which points to one person
- (o) Personally identifiable financial information
  - Account information – balance, history, details
- (p) Publicly available information
- (k)(2)(x) Financial institution includes real estate settlement service provider

11

Federal Law – 16 CFR Sec. 314

101

- Sec. 314.3 Standards for safeguarding customer information
  - Develop, implement & maintain comprehensive information security program
  - Written
  - Containing administrative, technical & physical safeguards
- Appropriate to
  - Size
  - Complexity of your activities &
  - Sensitivity of customer information at issue

12

Federal Law – 16 CFR Sec. 314.4 - Elements

- (a) Designate employee(s) to coordinate information security program
- (b) Identify foreseeable internal & external risks
  - Assess sufficiency of safeguards
    - Self-risk assessment
      - Employee training
      - IT systems
        - Processing, storage, transmission & disposal
        - Detecting, preventing & responding to attacks, intrusions or other failures

13

Federal Law – 16 CFR Sec. 314.4 - Elements

- (c) Design & implement information safeguards
  - Monitor
  - Test regularly
- (d) Oversee service providers
  - Selection
  - Requirement to comply with safeguards
- (e) Evaluate & adjust

14

Florida Law – Sec. 501.171, F.S.

- (1)(g) 1. Personal information
  - Name plus
    - Social security or other government issued number or
    - Financial account, credit card, debit card number with required security code, access code or password
    - Medical history
    - Health insurance policy number
- (2) Requirements for data security
  - Shall take reasonable measures to protect & secure data in electronic form containing personal information

102

15

Florida Rules of Professional Responsibility

- 4-1.6 Confidentiality of information
  - (e) Inadvertent disclosure of information –
    - Must make reasonable efforts to prevent inadvertent or unauthorized
      - Disclosure of, or
      - Access to
  - Acting competently to preserve confidentiality
    - Required reasonable efforts
    - Considerations of reasonableness
      - Sensitivity of information
      - Likelihood of disclosure
      - Cost of employing additional safeguards
      - Difficulty of implementing

113

16

Florida Rules of Professional Responsibility

- 4-1.6 Confidentiality of information – acting competently
  - Beyond scope - state & federal laws regarding privacy laws & notice of loss of information or unauthorized access
  - Transmitting information
    - Reasonable precautions
      - Prevent information coming into unintended recipients
      - No special steps needed, IF method affords reasonable expectation of privacy

17

Disposal of Consumer Information

107

- 16 CFR Sec. 682
  - Must take reasonable measures to protect against unauthorized access
  - Examples
    - Burning, pulverizing or shredding of papers – so cannot be reconstructed
    - Destruction or erasure of electronic media – so cannot be read or reconstructed
    - Use third party, but first must vet & monitor
    - Protect against unauthorized or unintentional disposal
    - Subject to Gramm-Leach-Bliley Act (16 CFR Sec. 314) – include disposal information into security program

18

ALTA's Best Practices

Pillar 3

Adopt & maintain a written privacy & information security program to protect

Non-public Personal Information

as required by local, state, & federal law

19

Assessment

By Category

20

Assessment

- Identification of potential threats – internal & external
  - Paper copy – someone taking a cellphone picture
  - Email – phishing or hacking
  - Working on a computer – someone looking over a shoulder
  - Disposal of information – someone re-constructing information

21

Assessment

- Risk – likelihood of it actually happening
  - Don't underestimate
    - Desperate people do desperate things
  - Has it happened to another Fund member?
  - Has it happened to someone you know?
  - Is it in the news?

22

Assessment

- Impact – if it happens
  - What happens to your business?
  - What happens to your clients?
  - What happens to your employees?

23

Assessment

- Steps to reduce risk
  - Paper information
    - Can parts be put back together?
  - Digital
    - Erasing is not enough – use a hammer
  - Privacy screens
  - Training
  - Training
  - Training
  - Oh did I mention training?

24

Assessment

- Steps in reaction – it happened – now what?
  - Phone list to make calls
  - Security
  - New work space
  - Notification
    - Law enforcement
    - Bank
    - Clients
    - Employees

25

Audit & Oversight

26

Audit & Oversight

- Audit – who performs
  - Self
  - Third party
    - Outside party to attempt to breach your security
      - Office
      - Computer
    - Report
    - Guidance

27

Audit & Oversight - Training

- Who is Audited
  - Employees
  - Vendors
- What is being evaluated
  - Policies & procedures
  - Prevention tactics
  - Identification something has gone wrong
  - Notification
    - Management
    - Clients
  - Next step

28

Audit & Oversight

- Review
  - Policies & procedures
- Observe
  - Employees
  - Vendors
- Test policies & procedures
  - Checking clients or vendors in
  - Giving name badges
  - Escorting in office
  - Penetration test
    - Network
    - Office

29

Audit & Oversight

- Review results
  - Self
  - Employees
  - Vendors
- Make adjustments to policies & procedures, if necessary
- Train
- Train
- Train

30

Procedure

- Test information systems to detect security risks, vulnerabilities & threats
  - Independent company – third party
    - Penetration test
- Review testing procedures
- Document
  - Testing - routinely
  - Results
  - Adjustments

31

Procedure

- Test results
  - Identify system failures
  - Identify unmanageable threats
    - Document
      - Each risk
      - Explain why risk cannot be managed

32

Documentation

33

Documentation

- Policies & procedures – include
  - Date of last review of same
  - Date of last update
- Training
  - Who
  - What
  - When
  - Where

34

Documentation

- Testing – Audits & Oversights – include
  - Date, type & who completed the audit
  - Results of the audit
  - Actions based on audit
    - Update of policies & procedures
    - Training
    - Reprimand

35

Documentation

- Risk mitigation efforts
  - How to keep the problem from getting worse
    - Shut down server
    - Remove computer from network
      - "Put the shovel down"
- Breaches
  - When
  - How
  - Reaction
  - Changes to prevent same in future

36

Documentation

- Notifications
  - Management
  - Employees
  - Vendors
  - Clients
  - Banks
  - Law enforcement
  - Other

37

Annual Review

Or Sooner

38

Annual Review

- Pillar 3 as with all Best Practices
- Reviewed at least annually
  - Update
  - Re-train
  - Re-acknowledge
- Incident may give rise to re-review
  - If no changes necessary
    - Note review was completed
- Set up pillars to review one per month
- Document review date

39

Third Party Requirements

40

Third-party Requirements

- Who
  - Lender
  - Insurance companies
  - Clients
- Obtain requirements
  - Written policy & procedures
  - E&O coverage
  - Security risk assessment
    - Frequency
      - Annually
      - Biannually

41

Security Risk Assessment

- AKA – penetration test
- Vendor to provide
- Review policy & procedure
- Test adherence to policy & procedure
  - By appointment
  - Surprise – remember no admittance to office without an appointment
- Attempt access to
  - Physical files
  - Digital files

42

Third-party Security Risk Assessment

- Receive a written report of testing results
  - Compliance with policy & procedure
  - Areas of concern
  - Areas needing improvement
  - Suggestions for changes to policies & procedures
- Many companies provide these services

43

Additional Steps

- Your own requirements may be most stringent
- Educate real estate agents & clients
  - Fraud
  - Targets
  - Email address

44

Digital Security

Network Systems

45

Assessment - Network

120

- Identification of potential threats
  - Hackers
  - Phishing
  - Spear phishing

46

Assessment - Network

- Risk – likelihood
  - The Fund receives calls everyday
  - Extremely high
  - Evidence of intrusion or attempt
    - Emails
      - Unsolicited for representation
      - Beneficiary of rich overseas prince
    - Computer
      - Working slowly
      - Pop-ups
      - Will not turn on
      - Missing

47

Assessment - Network

- Evidence of intrusion or attempt
  - Misdirected wire
  - Call or email to change type of payment
  - Call or email demanding something be “done right now”

48

Assessment - Network

- Impact
  - Loss of all electronic data
  - Computers damaged beyond repair
  - Financial loss
  - Complaint – even if not true
    - Bar
    - DFS
  - Distraction from business of law

49

Assessment - Network

- Steps to reduce risk – what did you do to prevent?
  - Policies & procedures
  - Training
  - Testing
    - In-house
    - Third party
  - Software – up to date
  - Firewalls – up to date
  - Anti-virus software – up to date
  - Computer hardware – up to date

50

Assessment - Network

- Steps in reaction
  - Remove infected computer from network
  - Shut network down
  - Notification to
    - Employees
    - Vendors
    - Clients
    - Lenders
  - Evaluation of what happened
    - Adjust policies & procedures
    - Train
    - Test

51

System - Type

- Smart desktops
  - Everyone saves own work
  - Each computer is independent
  - Most common – easy to find software
- Terminal services
  - Does not take advantage of each computer's power
  - Everyone works on a single computer via their terminal (computer)
  - One point to secure
  - Software is more difficult to find
  - Old school way – pre-personal computers
- Know what you have & how to secure

52

Router

- Router's name & password
  - Don't use the default
  - Set up separate access for guest
  - Set up password for each
  - Change password for each
    - Loyal Fund Office
      - Lindalik3scat$!&r3dwin3
      - FBI Mobile Unit #6565
    - Loyal Fund Office Guest
      - LFOgu3$tfall

53

Router

- Keep router software up to date
  - Can be automatic
  - Double check periodically – manufacture's website
    - IT professional can help
- Turn off remote management features
  - Hackers use this as an entry point
- Log out as administrator when not using
  - Hacker will try to piggyback in on a logged in administrator account

54

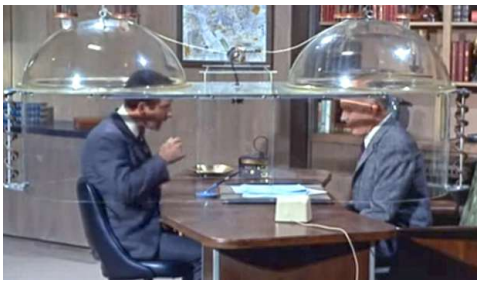
VPN – Working Outside the Office

- Virtual Private Network
  - Creates a private network from a public internet connection
  - Masks your internet protocol (IP address)
  - Online actions are virtually untraceable
  - Establishes secure & encrypted connections
    - More privacy
  - Prevents “eavesdropping”

55

VPN Hides

- Hides
  - Browsing history
  - IP address & location
  - Location for streaming
- Protects devices from eavesdropping hackers
  - Data sent
  - Data received



56

Document – All Steps

- Safeguard network connections
- Safeguard networks
- Mitigation efforts
- All changes in reaction to
  - Breach
  - Testing
  - Change in office
  - Change in law
  - Recommendations by third party

57

Audit, Oversight & Documentation

- Audit & Oversight
  - Train employees on procedure
  - Test systems & employees
  - Penetration test by third party
  - Work with third party for auditing

- Document
  - Procedures
  - Training
  - Testing
  - Testing results
  - Risk management efforts
  - Breaches
  - Notifications
  - Update to procedures
- Annual review

58

Procedure Example

- Network security –
  - Router has a two logon names, one for employees & one for guests
  - Router password shall contain at least 30 characters, including at least one capital letter & one special charter
  - The password is changed quarterly & when an employee has left our employment
  - Employees working remotely will have access to our network via VPN connection
  - Software & firewalls
    - Automatically updated &
    - Manually check for updates to be conducted at least quarterly

59

Procedure Example

- Network security – continued
  - The Firm sets up email accounts for employees to use during their employment with the domain name (closings@TheFirm.com; JSmith@TheFirm.com, etc.)
  - Employees are not allowed to use other email (gmail, yahoo, etc.) accounts for work
  - In-house testing of access to network is done quarterly
  - Testing of access to network is conducted by a third party bi-annually
  - Documentation of all updates (not specific password) shall be made
  - Documentation of any intrusion to network shall include steps to prevent further intrusions & notifications issued

60

Procedure Example

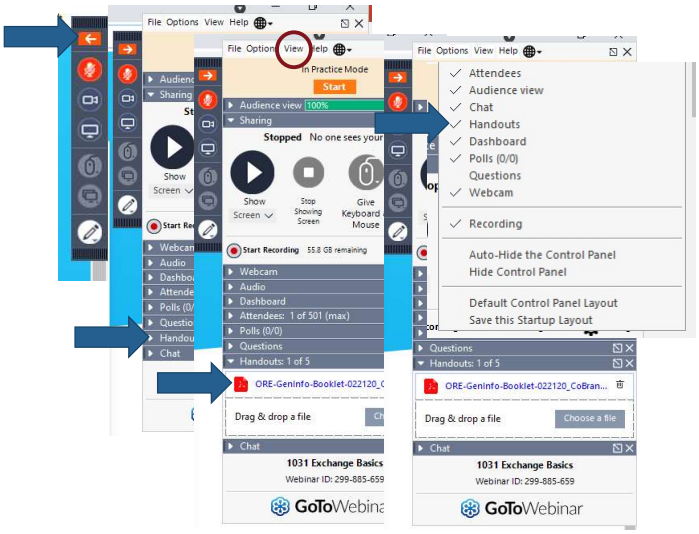
- Network security – continued
  - Any additional steps to mitigate loss of non-public personal information shall be documented
  - Employees shall be trained on network security at least semi-annually
  - Employee access to network, email & VPN will be terminated at the same time employment is terminated
  - Passwords will not be posted
  - Firewalls to block internet sites not necessary for office work (Amazon, YouTube, Facebook, etc.)
  - Keep network protected with current technology & software

61

End of Part 1

62

To Obtain Handout(s)



1. Locate control panel
2. Click red arrow
3. Find “Handouts:”
4. Click on the triangle
5. Click on the PDF
6. If you can’t see it click on “view” & make sure “Handouts” is checked

65

65

Protecting NPI – Pillar 3

Protecting Your Practice as You Protect Your Customers’ NPI:
An In-Depth Look at Best Practice Pillar 3 – Part 2

Linda Monaco, B.C.S.
Senior Legal Education Attorney

66

Parts 1 & 2

- Part 1
  - NPI
  - Assessment
  - Audit & oversight
  - Documentation
  - Annual review
  - Third party requirements
  - Digital security
- Part 2
  - Data security
  - Physical security
  - Disaster preparedness
  - Employees, vendors & third parties
  - Security breach notification

67

Digital Data Protection

68

Assessment – Digital Data

- Identification of potential threats
- Risk – likelihood – extremely high
- Evidence of intrusion or attempt
- Impact
  - Loss of money
  - Loss of clients
  - Distraction from business
- Steps to reduce risk – what did you do to prevent
- Steps in reaction

69

Digital Data

- In use
- In transmission
- In storage
- Disposal
- Security breaches
  - Monitor
  - Detect
  - Report
- Recovery plan

70

Data in Use

- Accessible to only those who need to know
  - Block or lock access by others
  - Real estate closing team to have access
  - Others (litigation paralegals, receptionist, etc.) no access
  - IT can help facilitate
    - Can block access to files on the server
- Evaluate each position to determine if access is needed
  - Ensure that background checks are performed on employees who have access

71

Passwords – Unique to each site

- If your common password is discovered
  - Will have access to all accounts which use that password

Passwords – Change Often . . . or Not

- Old rule – change often
  - Lead to issues, writing & posting, easy, re-used, month & date
- New rule – have better passwords & less changes
  - More compliance
  - Long passwords are strong passwords

72

Passwords – Use a Strong Password

- 12 characters minimum – the longer the better
- Mix it up – letters, numbers, symbols, uppercase, lowercase
- Don't use dictionary word or combination

Too Simple	Better
H0use	BigHouse$123
Cat in the Hat	Correct horse battery staple
My beautiful red house	Seashell glaring molasses invisible

- www.Diceware.com provides list of words
  - Roll your dice & create your passphrase

73

Password Manager

- Encrypted vault for login credentials
  - May also save
    - Notes
    - Insurance cards
    - Credit card information
- Issue security alerts
- Generate passwords
- Streamlines logins
- Break bad habits
  - Unique passwords
  - Change passwords

74

Password Managers

- LastPass
- Dashlane
- 1Password
- Keeper
- Sticky password
- Intel's True Key
- RoboForm
- Iolo Technologies
- EveryKey
- My PassLock

Remember there is NO FREE LUNCH!

75

Password Multipart Authentication Your Best Friend

- Process – How to know its really you
- Five common authentication factors
  - 1 Something you know
    - Password, address, other names, first car, etc.
  - 2 Something you have
    - Site sends a code or token which expires within a short time
  - 3 Something you are
    - Fingerprint, retina, iris, voice, face, etc.
  - 4 Somewhere you are
    - IP address – it knows your computer
  - 5 Something you do
    - Gestures or touches

76

Passwords – Tips

1. Don't use obvious personal information
2. Don't re-use passwords
3. Don't share your passwords – with ANYONE
   - Don't post your passwords
4. Use unique password for each site
5. Use password manager
6. Change your password regularly, or
   - Indication that you have been hacked
7. Use multi-factor authentication
   - Just turn it ON

77

All Electronic devices

- Computers, tablets, phones
- Privacy screen
  - Others in office
  - From outside the office
- Automatic lock device
  - After set time with no activity
- Automatic backup
- Train employees to lock when away from device

78

Data in Transmission

- Use current software & technology
- Connections – encrypt
  - Email is NOT secure & never will be secure
  - Use secure platform to communicate with clients & vendors
    - Email stating you have a message - login
  - Use encrypted platform for client to enter own information
- Encrypt information
- Restrict or block use of removable media
  - Thumb drives
  - CD
  - Floppies

79

Wire Fraud - Tips

125

- Educate all parties of the prevalence of wire fraud
  - Buyers
  - Sellers
  - Real estate agents
- Set up secure numbers – distrust numbers in emails
- Urgency indicates FRAUD – do it now!
- Inform parties of your wiring process
- Don't change plans
- Use ALTA Outgoing Wire Preparation Checklist

80

Data in Storage

- Encrypt
- Back up
  - Automatic
    - Frequency
      - Daily
      - Hourly
- Cloud – what security does it have
- Removable items
  - Who has access
    - Need to know
  - Location
    - Lock it up

81

Data Disposal or Sanitation

- Cloud
  - Determine if cloud provider allows for sanitation
  - Process for sanitation
    - By file
    - By group of files
    - Automatic
    - Request
  - Not available on all cloud systems
- Physical devices covered in physical data section

82

Recovery Plan

- "Houston, we have a problem . . ."
  - Clicked on the wrong item
  - Ransom call - ransomware
- What steps?
  - Who to call
  - What to do
  - How to get back to normal
- Train employees not to hide problem
- Notifications addressed in security breach section
- ALTA Rapid Response Plan for Wire Fraud Incidents

83

Audit, Oversight & Documentation

- Audit & Oversight
  - Train employees on procedure
  - Test systems & employees
  - Penetration test by third party
  - Work with third party for auditing

- Document
  - Procedures
  - Training
  - Testing
  - Testing results
  - Risk management efforts
  - Breaches
  - Notifications
  - Update to procedures
- Annual review

84

Procedures Example

- Delineate the company's acceptable use of technology
  - Facebook
  - Internet (shopping)
  - Personal emails
  - Information resources
- Employees to complete an annual acceptable use of information technology agreement
- Access to files with NPI is restricted to those who require access
  - Each position is evaluated to determine level of access

85

Procedures Example

- Review annually
  - Positions of employees & level of access to ensure access is appropriate
  - No unauthorized users have access to NPI
- Restrict use of removable storage devices
- Require passwords to open computers & files
  - Unique login identification
  - Unique passwords
- Restrict remote access
  - When remote access is warranted require use of VPN

86

Procedures Example

127

- Use third party to verify restricted access is working as intended
- Post privacy policy in office
  - Give copy of privacy policy to clients
  - Review privacy policy annually
- Have privacy policy available on website
- Privacy policy note
  - Personal information
    - Collected
    - Given &
    - Stored

87

Procedures Example

- Use wire transfer prevention tactics
- Train each employee on all of the procedures
- Employees to acknowledge training & understanding of procedures
- Communication with clients will be encrypted or via email with instructions to logon to encrypted safe platform
- Records will be stored & maintained according to Florida law
- Records will be destroyed in accordance with federal, state & local law
  - Record Retention & Disposal: Put It in Writing – on-demand webinar

88

Physical Security

Items Containing NPI

89

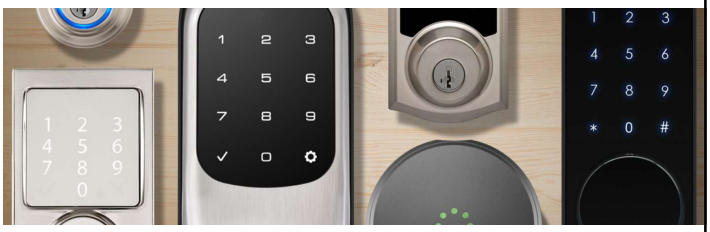
Access by People

- Intentional
  - Thieves
- Unintentional
  - Curious
- Employees
  - Only employees who require access for their job – need to know
  - Some will have access, some will not
- Visitors
  - Clients
  - Third-parties

90

How to Limit Access by People

- Lock the front door
- Appointment only
- Visitors to
  - Sign in
  - Wear name badges
  - Be escorted by employee at all times in the office
- Notify employees of a visitor in the office
- Use screen covers on monitors
- Employees should not be able to see each other's monitors



91

Clean Desk – Everyone!

- Anyone can take a picture of NPI on a desk
- People can read upside-down
- All employees, temporary workers, third party vendors & vendors are subject to policy
- No files on desk or floor when another person is in office

92

Clean Desk – Everyone!

- No files on desk or floor when another person is in office
  - Use empty bookcase for file organization
  - Only meet visitors & employees (need to know) in conference room
- Files with NPI
  - Not to be left unattended (running out to lunch or bathroom)
  - Stored in a locked cabinet when not in use
- Computer
  - Screen blocker
  - Locked when away from desk

93

Clean Desk – End of Day

- Lock all physical files
- Log out of computer
- Lock computer
- Lock electronic devices (laptops, tablets, cellphones, etc.)
  - In cabinet or
  - Desk
- Lock mass storage devices (CD ROM, DVD, etc.)
- Lock removable media (thumb drives, CD, external hard drives)

94

Clean Desk – Implementation – Document

- Document each step:
  - Training employees
    - With written copy of procedures for employee
  - Obtain acknowledgment of
    - Training
    - Understanding
    - Agreement to follow procedures &
    - Receipt of written procedures
  - Monitor employees
    - Variances from procedures in personal file

95

Electronic Devices

- Computers
- Cellphones
- Tablets
- Laptops
- Fax machines
- Copiers
- Anything else used to access documents with NPI

96

Electronic Devices

- Screen proctors
- Password protected
- Timed automatic lock
- Access – need to know
- Lost or stole
  - Auto destruct – find my device app installed

97

Electronic Device Replacement

- Cellphone
  - Do not allow store employee will move information
  - Old cellphone
    - Wiping is not be enough
    - Restoring factory settings is not enough
- Computers, tablets, fax & copiers (yes, copiers)
  - Erasing data is not enough
  - Wiping is not enough
  - Need a hammer

98

Conference Room – Closing Table

- Who attends
  - Buyers
  - Others to whom buyer has given express signed written permission
    - Real estate agents
    - Friends

99

Movement of Physical Data

- Does the document really need to be sent somewhere?
- Take precautions so that NPI cannot be read through envelope
- Track documents containing NPI

100

Storage of Physical Data

- Warehouse or document custodian
  - Secure
  - Who has access
  - What is their disaster plan
    - Fire
    - Water
    - Wind
  - What is their insurance

101

Storage of Physical Data

- Archive System
  - Convert physical to digital
    - Cloud
  - Convert to other physical
    - CD
    - Tape
    - Thumb drives
    - Removal Hard drives
  - Who has access
  - Location

102

Destruction of Physical Data

- When to destroy – file dependent
- Shredding company
  - Locked shredding collection bins
  - On site shredding – employee supervise
  - Off site shredding
  - E & O
  - How are their employees screened
  - Agreement to protect NPI
- Self-shredding
  - At each desk or central location
  - Adequate shredding

103

Audit, Oversight & Documentation

- Audit & Oversight
  - Train employees on procedure
  - Test systems & employees
  - Penetration test by third party
  - Work with third party for auditing

- Document
  - Procedures
  - Training
  - Testing
  - Testing results
  - Risk management efforts
  - Breaches
  - Notifications
  - Update to procedures
- Annual review

104

Procedure Example

- Limit access to physical locations of NPI
  - Building
  - Office
  - Desk
  - Computer
  - Storage
- Lock up files with NPI
- Clean desk
- When away from desk
  - Lock computer
  - Lock files with NPI
- Only employees who need information to have access
  - Need to know

105

Disaster Preparedness

106

Disaster Preparedness

- AKA Business continuity & disaster recovery plan
- Assessment – what type of disasters & possibility of affecting business
- You evaluate
  - Threats
  - Probability &
  - Severity
- Kind of disasters
  - Pandemic
  - Hurricane
  - Fire
  - Flood
  - Earthquake
  - Tornado
  - Civil unrest/terrorism/war
- Plan for each kind

107

Interruption or System Failure

- Power outage
- Internet loss
- Server outage
- Computer issues
- Storage issues
- Data issues

108

Resumption of Business – Overwhelming!

- Office building
- Everything in the office
- IT
- Employees
- Employees' families
- Clients
- Vendors
- Finances
- Insurance
- Security
- Electricity
- Internet access
- Internet presence
- Communication
- Data
- Mail

109

Overwhelming!

110

Tips

- Key functions vs. other functions
- Review business practices for streamlining
- Set up teams
  - Person to monitor warnings & alerts
- Separate plan for type of disaster
- Supplies needed
  - Timing for acquisition
- List of help – contacts & numbers
- Inventory
- Finances
- Training & testing

111

Resources

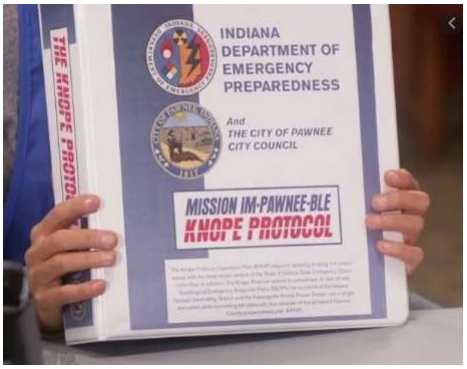
- www.usa.gov/prepare-for-disasters
  - Re-directs to Ready.gov
- Ready.gov
  - Department of Homeland Security
- www.floridadisaster.org/business/planning-for-business
  - Florida Division of Emergency Management
  - Re-directs to Ready.gov
- www.ibhs.org
  - Insurance Institute for Business & Home Safety
- www.disastersafety.org
  - Insurance Institute for Business & Home Safety

112

Where to begin

- Review OFB-EZ, Stay Open for Business
  - 20 pages
  - Reviews
    - Operations
    - Employees
    - Clients
    - Vendors
    - IT
- Establish team
  - One task at a time
  - Draft, test & review
  - Dry runs (fire drill)

130



The Fund

113

OFB-EZ

Know Your Operations

Use this form to identify what business functions are critical to your business' survival. Duplicate the form for each business function.

Updated:
Next Review Date:

BUSINESS FUNCTION:

Priority: ☐ Extremely High ☐ High ☐ Medium ☐ Low

Employee in charge:
Timeframe or deadline:
Money lost (or fines imposed) if not done:
Obligation: ☐ None ☐ Legal ☐ Contractual ☐ Regulatory ☐ Financial

Who performs this function? (List all that apply)
Employees:
Suppliers/vendors:
Key contacts:
(For additional space, use the Notes area below)

What is needed to perform this function? (List all that apply)
Equipment:
Special Reports/Supplies:
Dependencies:
(For additional space, use the Notes area below)

Who helps perform this function? (List all that apply)
Employees:
Suppliers/vendors:
Key contacts:
(For additional space, use the Notes area below)

Who uses the output from this function? (List all that apply)
Employees:
Suppliers/Vendors:
Key Contacts:
(For additional space, use the Notes area below)

Brief description of how to complete this function:

Workaround methods:

Notes:

OFB-EZ™ is a program of the Insurance Institute for Business & Home Safety 7

OFB-EZ

Know Your Employees

Use this form to record information about all employees, including the business owner so that each person can be contacted at any time. Duplicate the form for each employee.

Updated:
Next Review Date:

EMPLOYEE NAME:

Position/title:
Home address:
City, State, ZIP:
Office phone: Ext. Alternate phone:
Home phone: Mobile phone:
Office e-mail:
Home e-mail:
Special needs:

Certifications:

☐ First Aid ☐ Emergency Medical Technician (EMT) ☐ CPR ☐ Ham Radio
☐ Other:
☐ Special licenses:

Local Emergency Contact

Full name:
Relationship:
Home phone: Mobile Phone:
E-mail:

Out of State Emergency Contact

Full name:
Relationship:
Home phone: Mobile Phone:
E-mail:

Notes:

OFB-EZ™ is a program of the Insurance Institute for Business & Home Safety 9
Download this document at DisasterSafety.org/ibhs-in-business

114

Severe Weather Emergency

150

- EZ-Prep

Natural Disaster	Seasons	Geographic Location
Severe Winter Weather	Nov. 1–Mar. 1	Northeast, Midwest, Mountain West, Northwest, High elevation in Southeast and Mid-Atlantic
Flooding	Mar. 1–June 30	Northwest, Mountain West, Northwest, Midwest
Flash Flooding	Year-round	Nationwide
Tornadoes	Mar. 1–June 30	Midwest, Southeast, Southwest, Mid-Atlantic
Hurricanes	June 1–Nov. 30	Gulf Coast and Atlantic Seaboard States
Thunderstorms and Lightning	Mar. 1–Sept. 30	Central Plains, Southeast, Mid-Atlantic, Southwest
Hailstorms	Mar. 1–September 30	East of the Rockies
Wildfire	Mar. 1–June 1	Southeast
	June 1–Nov. 1	Mountain West, Pacific West, Southwest

115

Help for Businesses

- Employees
  - How to report for work
  - Do they have what they need
    - Food
    - Water
    - Cash
  - Where they will work
- Secure office & contents (fire)
  - Fences
  - Security

STAY OPEN OFB-EZ FOR BUSINESS®
A PROGRAM OF IBHS

116

Help for Business

- How to get up & running again
  - Notification to
    - Employees
    - Clients
  - Mobile office
  - Electricity
  - Internet access
  - IT
  - Data

STAY OPEN OFB-EZ® FOR BUSINESS
A PROGRAM OF IBHS

The Fund

117

Regular Testing

- Fire drill
- Active shooter test
- Verify vendors are ready
- Test employees for readiness
- "This is just a test – if it had been a real emergency, you would have been told . . ."

The Fund

118

Audit, Oversight & Documentation

- Audit & Oversight
  - Train employees on procedure
  - Test systems & employees

- Document
  - Procedures
  - Training
  - Testing
  - Testing results
  - Risk management efforts
  - Update to procedures
- Annual review

119

Procedure - Include

- Protection against damage or loss of information in event of disaster
- Address any interruption or failure of systems or equipment
- Business resumption post disaster
- Testing on a regular basis with documentation of same
- Review annually

120

Employees & Non-employees

121

Employees - Assessment

- With access to NPI or trust funds
  - Five-year background check prior
    - First day of work
    - Promotion
  - Update every three years
    - Calendar as an automatic reminder
- Documentation
  - Keep evidence of same
    - Invoice or
    - Documentation in personnel files

122

Employees

- Specific training for protection & security of NPI
  - Secure in use
  - Secure in storage
  - Secure disposal
- No “ride-along” – take your child to work
- Passwords
  - For all systems
  - Protected – not posted

123

Employees – Maintenance

- Ensure access to NPI is on an as needed basis
- Annually review each employee’s access to determine if access is still warranted
  - Adjust access as needed
- Terminate employee’s access upon separation from company or change in position
  - Employee separating from company will have access to physical & digital items terminated on the same day as separation
- Document each change in access
- Annually test 5 files or 10% to ensure access was terminated
- Review policy annually

124

Non-employees

- Non-employees who might have access to
  - Office &/or
  - Digital information

Examples

- Clients
- Housekeeping
- Shredder pickup
- Exterminator
- Repair person
- Building management
- Maintenance
- IT professional

125

Non-employees

- Assessment
  - What exposure of NPI
  - Possible damage due to such exposure
- Audit & Oversight
  - Background check – review from their employer
    - Document file on company
  - Inform of other policy & procedures
  - Observe others for compliance
    - Document any non-compliant behavior
- Review policy & procedure annually

126

Non-employees

- Set standards for entering office
  - Appointment required
    - No – walk in
      - Vendors for sales
      - Clients
  - Sign in at front desk
    - Check ID
  - Name tag

127

Non-employees

- Physical access
  - Escorted during entire stay or
  - All NPI locked away
    - View
      - On desk &/or
      - On computer, etc.
- Digital access
  - Only by
    - Employees &
    - IT professional
  - No guest privileges

128

Non-employees

- Share copy of policy & procedures
- Obtain
  - Signed acknowledgment & agreement to follow policy & procedures
  - Copy of E&O
    - Updated as E&O expires

129

Audit, Oversight & Documentation

- Audit & Oversight
  - Train employees on procedure
  - Test employees
  - Penetration test by third party
  - Work with third party for auditing

- Document
  - Procedures
  - Training
  - Testing
  - Testing results
  - Risk management efforts
  - Update to procedures
- Annual review

130

Procedure Example – Employee

- Review employee's background to minimize risk at time of hire, every 3 years & upon promotion
  - Keep documentation of same in employee's personal file
  - Calendar for future checks
- Train employees in protecting & safeguarding client's NPI while in use, in storage & at disposal
- Sample testing for background checks, completed training & change of access annually unless circumstances warrant additional testing
  - Testing pool shall be at least 5 files or 10% of all employees, which ever is larger

131

Procedure Example – Non-employee

- Review & document background checks of any person who has access to NPI, unsecured, unsupervised office & digital files
- Only non-employees with appointment will be allowed access to the office
- Inform non-employees on proper documentation needed for access to office (company picture ID)
- Non-employees to sign-in at the front desk & always wear the assigned name tag
- When possible non-employees shall be escorted during their visit to the office

132

Procedure Example – Non-employee

- Non-employees shall be given a copy of the policies & procedures to ensure compliance
- Non-employees are required to sign acknowledgment of receipt of policies & procedures
- Non-employees will provide written assurances of compliance with the policies & procedures
- Non-employees will provide written assurances of following their own policies & procedures in regard to background checks, audits, security reviews, intrusion logs & other evaluations

133

Security Breach Notifications

134

Sec. 501.171, F.S.

169

- Breach
  - Unauthorized access of electronic data containing personal information
- Covered entity
  - Entity which acquires, maintains or stores personal information
- Requires written notification of breach within 30 days to:
  - Individuals
  - Department of Legal Affairs, if more than 500 individuals compromised
  - Consumer reporting agencies if more than 1000 individuals compromised
  - Police – may need to provide police report

135

Florida Law – Sec. 501.171, F.S.

- No notification necessary if after consultation with relevant federal, state or local law enforcement agencies it is determined breach not likely to result in identity theft or harm
  - Retain the written determination for 5 years
  - Provide Department of Legal Affairs with written determination within 30 days after determination
- Late notifications subject to fines from
  - $1,000 per day
  - $50,000 for 30 day's late with
  - Maximum $500,000

136

Notice

- Written notice sent
  - To mailing address of individual or
  - Email to email address
- Minimum contents of notice:
  - Date, estimate date or estimate date range of breach
  - Description of personal information that was or reasonably believed to have been accessed
  - Contact information of covered entity
  - Personal information the covered entity maintained about individual

137

Notice

- If over 1,000 individuals as a single time are compromised
  - Without reasonable delay notify all consumer reporting agencies
    - For details see, Fair Credit Reporting Act, 15 U.S.C.Sec. 1681 a(p)
- If notice is to over 500,000 see Sec. 501.171 (4)(f), F.S.
- If a third-party agent is used for storage & they are breached
  - Third-party agent shall notify within 10 days
  - Covered entity must still comply with notices & timing as discussed above

138

Audit, Oversight & Documentation

- Audit & Oversight
  - Train employees on procedure
  - Test employees
  - Work with third party for auditing

- Document
  - Procedures
  - Training
  - Testing
  - Testing results
  - Risk management efforts
  - Breaches
  - Notifications
  - Update to procedures
- Annual review

139

Procedure Example

- Monitor
  - Usually part of the operating system
  - May need enhancements
- Detect
  - Unauthorized access
  - Strange activity
    - Large file download
    - Time of activity
    - Permission changes
    - Processing

140

Procedure Example

- Action
  - Lock user activity – automatically
  - Close internet access
- Report breaches
  - Train employees
    - To look for “odd” items which may indicate a breach &
    - Steps to take if suspect breach
- Sample testing management follow up of activity on 5 – 10% which ever is greater (minimum of 25) files

141

Thank you

for your time and attention

For more information please contact:

Linda Monaco, B.C.S.

Lmonaco@TheFund.com

142

ALTA Best Practices Framework:

Assessment Procedures

Version 3.0

Final Draft

ALTA Best Practices Framework

The ALTA Best Practices Framework has been developed to assist lenders in satisfying their responsibility to manage third party vendors. The ALTA Best Practices Framework is comprised of the following documentation needed by a company electing to implement such a program.

- ALTA Best Practices Framework: Title Insurance and Settlement Company Best Practices
- ALTA Best Practices Framework: Assessment Procedures
- ALTA Best Practices Framework: Certification Package (Package includes 3 Parts)

Version History and Notes

Date	Version	Notes
7/19/2013	2.0	Publication of the ALTA Best Practices Framework: Assessment Procedures, along with other documents in the ALTA Best Practices Framework, as approved by the ALTA Board on July 19, 2013. This is the first publication of the ALTA Best Practices Framework: Assessment Procedures.
11/13/2014	2.1	Amendment to Assessment Procedure 3.09(a) pursuant to a motion approved by the Board of Governors to remove the reference to encryption of data at rest.
10/7/2016	2.5	Publication of the revised ALTA Title Insurance and Settlement Company Best Practices (including addition of third-party signing professionals provision), along with other documents in the ALTA Best Practices Framework, approved by the ALTA Board of Governors on September 19, 2016.
10/17/2019	3.0	Publication of the revised ALTA Title Insurance and Settlement Company Best Practices, along with other documents in the ALTA Best Practices Framework, approved by the ALTA Board of Governors on June 6, 2019.

Please Note

Utilize these ALTA Best Practices Assessment Procedures to determine compliance with the ALTA Best Practices. For Assessment Procedures with no defined sample size or tolerance, 100% compliance with each Assessment Procedure tested is required to be considered "Optimized." For Assessment Procedures with defined sample sizes and tolerance levels, results must be within the tolerance level to be considered "Optimized." If all Assessment Procedure results are "Optimized," then agent is fully compliant with the ALTA Best Practices. If results are not "Optimized" for any Assessment Procedure, refer to the ALTA Best Practices Maturity Model to develop a progress plan.

Capitalized Terms:

- Capitalized Terms appearing in both these Assessment Procedures and the ALTA Title Insurance Settlement Company Best Practices (Best Practices) shall have the meanings set forth in the Best Practices document.

Documentation Guidelines:

- Detailed notes or documentation copies should be maintained for a minimum of five (5) years to support testing performed and testing exceptions for each procedure.

Testing Guidelines:

- Where possible, the same file sample may be used throughout the assessment to test multiple attributes.

Not Applicable (NA):

- Some of the Assessment Procedures will not be applicable to some agencies due to laws, regulations, or business model. Inapplicability of an Assessment Procedure does not result in a "No" in the Optimized column for such procedure.

Assessment Procedure Number	ALTA Best Practices Framework: Assessment Procedures	Optimized (Y / N)
	ALTA Best Practice 1: **Establish and maintain current License(s) as required to conduct the business of title insurance and settlement services.**	
1.01	Obtain an understanding of the Company's process for monitoring and tracking the current License(s) as required to conduct the business of title insurance and settlement services.	Y / N
1.02	Confirm the active status of the Company and/or individual Licenses/registrations for each state in which the Company conducts business. In states where underwriter appointments are required, ensure that companies and/or individual producers are appointed by each underwriter as applicable. Documentation reviewed may include actual licenses, Department of Insurance or appropriate state regulatory agency websites/screenshots, Bar Association status, corporate, business registrations, or evidence of appointments with the state and other documentation as applicable to state/license. Sample Selection: • For each file selected in Assessment Procedure 4.03, verify that the Company maintains appropriate current and valid license(s) View Company's active ALTA Policy Forms License or verify compliance on ALTA website.	Y / N
1.03	View Company's active ALTA Policy Forms License or verify compliance on ALTA website.	Y / N
1.04	For each Company office location performing settlement services, verify the listing in the ALTA Registry (subject to those business entity types supported by the ALTA Registry).	Y / N

Assessment Procedure Number	ALTA Best Practices Framework: Assessment Procedures	Optimized (Y / N)
	ALTA Best Practice 2: **Adopt and maintain appropriate written procedures and controls for the protection of Escrow Trust Accounts allowing for electronic verification of reconciliation.** *Note: These procedures apply to all custodial or fiduciary accounts, including closing and disbursement accounts, recording and tax accounts, construction disbursing accounts, underwriter remittance/premium accounts and other similar accounts.*	
2.01	Obtain Company's written procedures and controls for Escrow Trust Accounts, hiring and training, and, at a minimum, verify all sections of ALTA Best Practice 2 are included.	Y / N
2.02	Obtain a complete listing, certified by Company, of ALL open (active and inactive; escrow and non-escrow) bank accounts and authorized signers/ wire initiators and approvers on the accounts. Sample Selection: Select a minimum sample of 5 or 10%, whichever is greater, of authorized signers on Escrow Trust Accounts (maximum of 25). If total population is less than 5, select 100%. Perform the following: a. Compare against the active listing of employees to verify all signers, wire initiators and approvers are actively employed. b. If signatory stamps are being used to sign escrow checks, test to confirm only authorized signers have access to the stamp. c. Obtain evidence (invoice/documentation in personnel files, etc.) that 5 year Background Checks were conducted upon hiring or within the past 3 years. d. Verify compliance with the Company's process for training employees on management of escrow funds and Escrow Trust Accounts.	Y / N If any exception is noted for any sub-procedure, answer "No."

Assessment Procedure Number	ALTA Best Practices Framework: Assessment Procedures	Optimized (Y / N)
2.03	Obtain two month end Three-Way Reconciliations for each Escrow or Trust Account and perform the following: *Note: Three-Way Reconciliation documentation at a minimum includes bank statement, reconciliation sheet/summary page with book balance, outstanding deposits list/deposits in transit, open escrow file listing or trial balance and outstanding disbursements list, all as of the reconciliation date. All amounts should equal between the book balance, reconciled bank balance and trial balance*. Definition of Significant items: ♦ Individual transactions/file balances over $10,000 over 10 business days old. ♦ Deposits in transit over $10,000 over 3 business days old. ♦ Aggregate transactions over $10,000 for shortages. ♦ Outstanding checks depending on payee as noted in sub-procedure 2.03.k in excess of $5,000 over 180 days old, mortgage payoffs over 10 business days old. Definition of Active versus Inactive/Dormant Accounts: ♦ Active Account - Used for current transactions. ♦ Inactive/Dormant Account ▪ No new incoming funds into account. ▪ No disbursements related to new closings from account. ▪ No activity through account in last six months (dormant). Sample Selection: ♦ Two months reconciliations for ALL Escrow Trust Accounts (also maintain for documentation). ♦ For a Company performing more than 100 transactions per month, perform sub-procedures 2.03.a through 2.03.f for all accounts for at least one of the two months. a. Verify that reconciliations were completed monthly and within 10 business days of the closing date of the bank statement. b. Verify that daily reconciliations of the receipts and disbursements and monthly Three-Way Reconciliations are	Y / N If any exception is noted in an individual sub-procedure, answer "No."

Assessment Procedure Number	ALTA Best Practices Framework: Assessment Procedures	Optimized (Y / N)
	prepared independently by someone not associated with the receipt and disbursement function. The daily reconciliation of the receipts and disbursements is not applicable to Inactive/Dormant Accounts. c. Verify that reconciliations are reviewed and signed off by management or a supervisor. d. Verify that reconciliations, bank statements and supporting documentation can be provided electronically to the Company's contracted underwriters upon request. e. Determine whether accounts are in balance, contain all supporting reports and that a proper three-way reconciliation is being produced. The book balance, reconciled bank balance and trial balance should be in agreement. f. Verify that the bank statements and account related documentation for each Escrow Trust Account is clearly labeled by the bank as an Escrow Trust Account and that the escrow checks and deposit tickets/records clearly identify the associated file numbers. g. Verify that for inactive/dormant accounts, senior management approval is required for any disbursement of funds. Sample Selection: ♦ For a Company performing 100 or more transactions per month, the following additional procedures must be performed on a sample of accounts representing at least 50% of the total number of accounts. ♦ For a Company performing fewer than 100 transactions per month, the following procedures must be performed on 100% of the total number of accounts. h. Agree opening bank and book balances to ending balance on prior month's reconciliation or differences are identified. i. Review bank statement activity noting bank charges, insufficient funds charges, negative daily balances, investigate and confirm resolution. Verify that all bank charges are funded by the Company's operating account within 5 business days of the earlier of discovery or completion of reconciliation. j. Test Significant deposits in transit listed on the most current reconciliation. If they are older than 3 business days, investigate and determine if there is a true shortage and verify resolution or funding.	

Assessment Procedure Number	ALTA Best Practices Framework: Assessment Procedures	Optimized (Y / N)
	k. Determine Company's process for follow up on outstanding checks, including procedures for escheating funds. Verify clearing or adherence to follow-up process for significant outstanding checks including but not limited to checks to recording clerk, tax collector, hazard insurance checks, underwriter checks or checks for mortgage payoffs and any other high risk items. l. Review the Trial Balance for dormant funds that may be eligible for escheatment to ensure Company is following its procedures. Test significant file shortages, dormant funds (significant file balances over 180 days) and significant miscellaneous files to verify documentation of their status and that shortages were funded within 5 business days of the earlier of discovery or completion of reconciliation. m. Review and test adjustments (reconciling items) needed to bring the account in balance and verify their validity. n. Verify that the Company is not comingling fiduciary funds, including the underwriter's portion of the premium, with operating funds. o. From a review of cancelled checks or disbursement registers, select a sample across accounts and test checks, if any, and wires that may require further review, such as checks going back into escrow, disbursements paid to cash or employees, amounts transferred between accounts, suspicious payees, multiple disbursements to the same payees, large round dollar amounts and any other questionable disbursements. These disbursements should be agreed to a closing file and settlement statement. p. Select a sample of three business days within the assessment period for the active escrow funding/settlement/disbursement accounts and verify agent is performing, at a minimum, a daily reconciliation of the receipts and disbursements.	
2.04	If the Company is holding any customer investment accounts, select a sample of interest-bearing trust accounts. Select a minimum of 5 or 10% of all interest bearing escrow or trust accounts, whichever is greater, (maximum of 25). If total population is less than 5, select 100%. Verify that the Company maintains records/documentation supporting activity for interest bearing (customer investment) escrow accounts.	Y / N If exceptions are noted in 20% or more of items, answer "No."

Assessment Procedure Number	ALTA Best Practices Framework: Assessment Procedures	Optimized (Y / N)
2.05	For ALL Escrow Trust Accounts, determine whether the Escrow Trust Accounts are maintained at Federally Insured Financial Institutions unless directed by the beneficial owner.	Y / N
2.06	For accounts reviewed in Assessment Procedure 2.03, verify the following: a. That the Company utilizes Positive Pay or Reverse Positive Pay on active accounts, if available in the local marketplace. Review bank documentation such as monthly account analysis statement or bank positive pay entitlement documentation. b. The Company has policies and procedures in place that prohibit or control the use of ACH and international wire transfers to protect against unauthorized transactions.	Y / N If any exception is noted in either sub-procedure, answer "No."
2.07	For wire activity: a. Obtain the Company's written wire transfer procedure and verify that it (1) includes verification of wire transfer instructions independent of initial communication for outgoing wire transfers; (2) for incoming wire transfers, a procedure to alert consumers regarding the risks of wire fraud and guidelines to mitigate losses; and (3) is tested at least annually. b. Obtain the Company's written wire fraud response procedure and verify that it substantially conforms to the ALTA Rapid Response Plan and is updated at least annually.	Y / N If any exception is noted in either sub-procedure, answer "No."

Assessment Procedure Number	ALTA Best Practices Framework: Assessment Procedures	Optimized (Y / N)
	ALTA Best Practice 3. **Adopt and maintain a written privacy and information security program to protect Non-public Personal Information as required by local, state and federal law.** *Note: These Assessment Procedures should be applied as appropriate to the Company's size and complexity, the nature and scope of the Company's activities, and the sensitivity of the Non-public Personal Information the Company handles.*	
3.01	Obtain the Company's information security program to protect its Non-public Personal Information and verify that the program is reviewed and updated as necessary, at least annually. The program should at a minimum ensure all sections of ALTA Best Practice 3 are included.	Y / N
3.02	Select a minimum sample of 5 or 10%, whichever is greater, of employees (maximum of 25). If total population is less than 5, select 100%. Obtain evidence that employees were trained in the Company's information security program to protect Non-public Personal Information.	Y / N If exceptions are noted in 20% or more of items, answer "No."
3.03	Obtain the Company's information security risk assessment, including the risk ranking of information systems. Review the Company's process for assessing risk to its customer information and verify that it includes the following: a. Locations, systems, and methods for storing, processing, transmitting, and disposing of its customer information. b. Potential internal and external threats that could result in unauthorized disclosure, misuse, alteration, or destruction of Non-public Personal Information or customer information systems and assessments of the likelihood and potential damage to the Company and its customers of these threats.	Y / N If no written Information Security Risk Assessment, answer "No."

Assessment Procedure Number	ALTA Best Practices Framework: Assessment Procedures	Optimized (Y / N)
3.04	Verify that key controls, systems and procedures of the information security program are regularly tested by qualified independent staff in accordance with the risk assessment. Specifically, review that the following are included in the testing: a. Management's documented approach for testing the information security program and evidence of testing. b. Frequency of testing of the information security program. c. Documentation of approach for tracking and remediating exceptions and/or control gaps.	Y / N
3.05	Verify employees are required to complete an acceptable use of information technology assets agreement at least annually (e.g., acceptable use of the Internet, email, and Company information resources). For the sample of employees tested in Assessment Procedure 3.02 above, review the signed Acceptable Use Policy.	Y / N If exceptions are noted in 20% or more of items, answer "No."
3.06	Obtain and review written policies and procedures to verify logical access to information systems (i.e., network, data base, and application layers) containing Non-public Personal Information is restricted to authorized persons only.	Y / N

Assessment Procedure Number	ALTA Best Practices Framework: Assessment Procedures	Optimized (Y / N)
3.07	a. Select a minimum sample of 5 or 10%, whichever is greater, of employees with access to NPI (maximum of 25). If total population is less than 5, select 100%. o Test the user access provisioning process to determine if access is approved in accordance with policy prior to granting. o Obtain evidence (invoice/documentation in personnel files, etc.) that 5 year Background Checks were conducted upon hiring or within the past 3 years. b. Select a sample of 5 terminated employees or 100% if less than 5 within the assessment period. o Verify the user access de-provisioning process to determine if access for terminated employees was removed per policy. c. Verify administrative access rights (i.e., ability to add, modify and remove user access) to systems containing Non-public Personal Information are not assigned to personnel performing business transactions within the system. d. Verify access review is being performed by management at least annually to confirm that only required employees have access to customer information or customer information systems necessary to perform job functions. e. Verify that logical access controls (e.g., unique User ID's, complex passwords, etc.) to the network and information systems containing Non-public Personal Information are in place. o Obtain listing of user ID's for systems with Non-public Personal Information. Verify ID's are unique and assigned to specific users. o Test password configuration controls in accordance with policy.	Y / N If exceptions are noted in 20% of items tested in sub-procedures 3.07.a or 3.07.b, answer "No." If any exceptions are noted in sub-procedure 3.07.c, 3.07.d, or 3.07.e, answer "No."
3.08	a. Review policies restricting or controlling the use of removable media (e.g., the use of USB ports, CD/DVD writable drives, etc.). b. Obtain evidence that system configuration settings are consistent with the policy.	Y / N

Assessment Procedure Number	ALTA Best Practices Framework: Assessment Procedures	Optimized (Y / N)
3.09	Determine if the Company utilizes encryption or a secure delivery method for Non-public Personal Information. • Obtain evidence demonstrating the use of encryption or alternative secure delivery method for Non-public Personal Information.	Y / N
3.10	a. Obtain and review documented procedures for monitoring, detecting attacks/intrusions into customer information systems, and responding to incidences. If monitoring of external threats has been outsourced, obtain evidence of reporting and subsequent management review. b. Select a sample of notifications of security alerts and verify management's follow-up activity. c. Obtain and review documented procedures for security breach notification, including evidence of program review at least annually.	Y / N If any exception is noted in an individual sub-procedure, answer "No."
3.11	a. Obtain and review the clean desk policy and verify compliance through inspection. b. Verify access to work areas and physical locations containing customer information, such as buildings, computer facilities and record storage facilities, is limited to authorized personnel only. Inspect physical locations to verify that they are secured and access is limited to authorized personnel.	Y / N If any exception is noted in an individual sub-procedure, answer "No."
3.12	a. Obtain and review change management procedures when technology and business function changes are made. b. Verify procedures are in place to determine that systems modifications (hardware and software) are consistent with the approved security program. Specifically, test a sample of hardware or software changes to verify that they are documented, tested and approved.	Y / N If any exception is noted in an individual sub-procedure, answer "No."
3.13	a. Obtain management's procedure for data and system backup and business resumption to protect against destruction, loss, or damage of information from potential environmental hazards, such as fire and water damage or technological failures. b. Verify that the disaster management plan is routinely tested with results documented.	Y / N If any exception is noted in an individual sub-procedure, answer "No."

Assessment Procedure Number	ALTA Best Practices Framework: Assessment Procedures	Optimized (Y / N)
3.14	Determine whether the Company provides Non-public Personal Information to any other party, including third-party signing professionals, or whether any other party has access to Non-public Personal Information through service provided directly to the Company. a. Verify and obtain evidence that Company conducted due diligence in selecting its service providers and taking information security into consideration. b. Verify that Company has controls to monitor security procedures of service providers to safeguard customer information (i.e., review the results of background checks, audits, security reviews or tests, intrusion logs, or other evaluations). c. If the Company has remotely-hosted or remotely accessible systems for storing, transmitting or transferring Non-public Personal Information, verify that the Company utilizes multi-factor authentication for all access points.	Y / N If any exception is noted in an individual sub-procedure, answer "No."
3.15	Verify the existence of Company's Privacy Policy and its process of giving notice to customers. If the Company does not have a website, ensure that notice is provided directly to customers in a usable format.	Y / N
3.16	Determine through inquiry of management whether the Company maintains a website. If so, inspect the Company's website and verify the following: a. The website includes the Company's Privacy Policy. b. The website's Privacy Policy accurately discloses what Non-public Personal Information is obtained on the site.	Y / N If any exception is noted in an individual sub-procedure, answer "No."
3.17	a. Obtain and inspect policies and procedures over record retention and disposal. Verify procedures are in place for disposal of Non-public Personal Information. b. If document/electronic media disposal services are provided by a third party, obtain evidence of the contract agreement/SLA and a recent document disposal certificate from the vendor.	Y / N If any exception is noted in an individual sub-procedure, answer "No."

Assessment Procedure Number	ALTA Best Practices Framework: Assessment Procedures	Optimized (Y / N)
	ALTA Best Practice 4 **Adopt standard real estate settlement procedures and policies that help ensure compliance with Federal and State Consumer Financial Laws as applicable to the Settlement process.**	
4.01	Obtain and/or document Company's written procedures to maintain compliance with established rates and legal and contractual requirements for recording documents and the use of third-party signing professionals and, at a minimum, ensure all sections of the ALTA Best Practice 4 are included.	Y / N
4.02	Select a sample of 5 files or 100% of closed files, whichever is less, during the assessment period and perform the following: a. Compare the settlement statement or Closing Disclosure and file ledger and investigate differences. Review closed file for supporting documentation for disbursements over $1,000 listed on the settlement statement. Investigate any unsupported disbursements. b. Verify disbursement and receipt dates and amount on the file ledger with the bank statement or copies of cleared checks, to determine timely clearance. Verify funds were received/ deposited prior to disbursement. c. For outgoing wire transfers, verify compliance with Company's policy for initiation and approval.	Y / N If exceptions are noted in 20% of items tested in any sub-procedure, answer "No."
Sample Selection: Instructions for Next Three Assessment Procedures	Sample Selection for Assessment Procedures 4.03 - 4.05: Based on Company's size, volume of business and process for title production, select a sample of closed files to test. The following should be considered when determining the sample: centralized vs. decentralized production, number of offices, number of closings, number of states in which the Company issues title policies, and the types of policies written (loan policies vs. owner's policies). Sample selection: • Minimum of 25 files or 100% of last 3 months of closed files, whichever is less.	

Assessment Procedure Number	ALTA Best Practices Framework: Assessment Procedures	Optimized (Y / N)
4.03	For sample selected as noted above, confirm the following: a. Documents were submitted or shipped for recording to the county recorder (or equivalent) or the person or entity responsible for recording within two (2) business days of the later of (i) date of Settlement, or (ii) receipt by the Company if Settlement is not performed by the Company. Documents are tracked and recording information retained. b. If recording was rejected, item was addressed within two (2) business days of receipt of the rejected documents. Documents and corrective actions, including resubmission, are tracked. In no instance should resubmission take more than 30 days.	Y / N If any exception is noted in 25% or more of items tested for any sub-procedure or if any one file takes more than 30 days to be submitted/ shipped/ resubmitted, answer "No."
4.04	For sample selected as noted above, perform the following: a. Test compliance with current filed or promulgated rates, endorsements, and/or rates established by the Company's title insurance underwriter(s) or rating bureau in each state, or Company rates in unregulated states, and where overpayments occurred, verify that refunds are issued upon discovery. b. Ensure discounted/reissue rates are calculated and charged when appropriate. c. Test transactions to determine whether non-title insurance rates for services provided by the Company agree with the Company's established rates. d. Document the Company's quality review process to ensure compliance with underwriter and/or agent established rates as determined by state law and where overpayment occurred, that refunds are issued upon discovery.	Y / N If any exception is noted in 10% or more of items tested for any sub-procedure, answer "No."

Assessment Procedure Number	ALTA Best Practices Framework: Assessment Procedures	Optimized (Y / N)
4.05	Within the file sample selected, review for use of third-party signing professionals, including notaries public, engaged by the Company and review for the following: a. Verify that the Company maintains a current copy of the third-party signing professional's (Notary's) Errors and Omissions insurance and if required by law, notary surety bond; b. Obtain evidence of the third-party signing professional's current state licensure, where required, or documentation that the third-party signing professional maintains a verifiable industry designation, if applicable; and c. Obtain evidence of the third-party signing professional's acknowledgement of compliance with Company's instructions and the Company's information security program, as detailed in Best Practice 3 of these Assessment Procedures. NOTE: If a third-party signing professional is directly employed by a title or settlement agent or underwriter that provides evidence of compliance with the Best Practices, the Company does not need to perform the requirements outlined in this section of the Best Practices Assessment Procedures. d. For such third-party signing professionals, verify that the third-party signing professional's direct employer is compliant with the Best Practices.	Y / N If any exception is noted in 20% or more of items tested for any sub-procedure, answer "No."

Assessment Procedure Number	ALTA Best Practices Framework: Assessment Procedures	Optimized (Y / N)
	ALTA Best Practice 5 **Adopt and maintain written procedures related to title policy production, delivery, reporting and premium remittance.**	
5.01	Obtain Company's written procedures and controls for title policy production, delivery, reporting and premium, and, at a minimum, ensure all sections of ALTA Best Practice 5 are included.	Y / N
5.02	Using the sample selected above for Assessment Procedure 4.03, perform the following: a. Verify title insurance policies are issued and sent to customer within 30 days of Settlement if terms and conditions of title insurance commitment have been satisfied. b. If terms and conditions of title insurance commitment were not satisfied at Settlement, verify policy was sent to the customer within 30 days from the date on which all terms and conditions of commitment were satisfied. c. Verify that policies are reported (including a copy of the policy, if required by the underwriter), in accordance with applicable statutory, regulatory and contractual obligations, but not to exceed 45 days after the later of (i) the date of Settlement, or (ii) the date that the terms and conditions of the title insurance commitment are satisfied. d. Verify that the correct portion of the premium collected was remitted to the underwriter in accordance with applicable statutory, regulatory and contractual obligations.	Y / N If any exception is noted in 10% or more of items tested for any sub-procedure, answer "No."

Assessment Procedure Number	ALTA Best Practices Framework: Assessment Procedures	Optimized (Y / N)
	ALTA Best Practice 6 **Maintain appropriate insurance and fidelity coverage.**	
6.01	a. Obtain a list of the Company's current professional liability insurance or errors and omissions insurance, cyber liability insurance, and crime coverage, fidelity coverage or surety bonds, including coverage amounts and expiration dates. Verify accuracy of the list by comparison to policy declaration pages. b. Verify that Company maintains professional liability insurance or errors and omissions insurance, fidelity coverage or surety bonds in accordance with the contractual agreement with the Company's underwriter. c. If coverage is required by state law, verify that coverage meets minimum requirements for each state in which the Company is licensed.	Y / N If any exception is noted for any sub-procedure, answer "No."

Assessment Procedure Number	ALTA Best Practices Framework: Assessment Procedures	Optimized (Y / N)
	ALTA Best Practice 7 **Adopt and maintain written procedures for resolving consumer complaints.**	
7.01	Obtain written policies and procedures for tracking and resolving consumer complaints. Verify that the following are included: a. A standard complaint form is utilized that identifies information that connects the complaint to a specific transaction and provides information to understand the nature and scope of the complaint. b. A single point of contact and/or department has been established for consumer complaints. c. Procedures have been established for forwarding complaints to appropriate personnel. d. A written log of consumer complaints is maintained that includes whether resolution is necessary and how resolved.	Y / N If any exception is noted in any sub-procedure, answer "No."
7.02	Obtain the consumer complaints log for a period of 1 year immediately preceding the assessment and verify that the Company followed the procedural guidelines for addressing complaints.	Y / N

§ 313.1 Purpose and scope.

(a) *Purpose.* This part governs the treatment of nonpublic personal information about consumers by the financial institutions listed in paragraph (b) of this section. This part:

(1) Requires a financial institution in specified circumstances to provide notice to customers about its privacy policies and practices;

(2) Describes the conditions under which a financial institution may disclose nonpublic personal information about consumers to nonaffiliated third parties; and

(3) Provides a method for consumers to prevent a financial institution from disclosing that information to most nonaffiliated third parties by ''opting out'' of that disclosure, subject to the exceptions in §§ 313.13, 313.14, and 313.15.

(b) *Scope.* This part applies only to nonpublic personal information about individuals who obtain financial products or services primarily for personal, family or household purposes from the institutions listed below. This part does not apply to information about companies or about individuals who obtain financial products or services for business, commercial, or agricultural purposes. This part applies to those ''financial institutions'' and ''other persons'' over which the Federal Trade Commission (''Commission'') has enforcement authority pursuant to Section 505(a)(7) of the Gramm-Leach-Bliley Act. An entity is a ''financial institution'' if its business is engaging in a financial activity as described in Section 4(k) of the Bank Holding Company Act of 1956, 12 U.S.C. 1843(k), which incorporates by reference activities enumerated by the Federal Reserve Board in 12 CFR 211.5(d) and 12 CFR 225.28. 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. 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, nonfederally insured credit unions, and investment advisors that are not required to register with the Securities and Exchange Commission. They are referred to in this part as ''You.'' The ''other persons'' to whom this part applies are third parties that are not financial institutions, but that receive nonpublic personal information from financial institutions with whom they are not affiliated. Nothing in this part modifies, limits, or supersedes the standards governing individually identifiable health information promulgated by the Secretary of Health and Human Services under the authority of sections 262 and 264 of the Health Insurance Portability and Accountability Act of 1996, 42 U.S.C. 1320d–1320d–8. Any institution of higher education that complies with the Federal Educational Rights and Privacy Act (''FERPA''), 20 U.S.C. 1232g, and its implementing regulations, 34 CFR part 99, and that is also a financial institution subject to the requirements of this part, shall be deemed to be in compliance with this part if it is in compliance with FERPA.

§ 313.2 Model privacy form and examples.

(a) *Model privacy form.* Use of the model privacy form in appendix A of this part, consistent with the instructions in appendix A, constitutes compliance with the notice content requirements of §§ 313.6 and 313.7 of this part, although use of the model privacy form is not required.

(b) *Examples.* The examples in this part are not exclusive. Compliance with an example, to the extent applicable, constitutes compliance with this part.

[74 FR 62965, Dec. 1, 2009]

§ 313.3 Definitions.

As used in this part, unless the context requires otherwise:

(a) *Affiliate* means any company that controls, is controlled by, or is under common control with another company.

(b)(1) *Clear and conspicuous* means that a notice is reasonably understandable and designed to call attention to the nature and significance of the information in the notice.

(2) *Examples*—(i) *Reasonably understandable.* You make your notice reasonably understandable if you:

(A) Present the information in the notice in clear, concise sentences, paragraphs, and sections;

(B) Use short explanatory sentences or bullet lists whenever possible;

(C) Use definite, concrete, everyday words and active voice whenever possible;

(D) Avoid multiple negatives;

(E) Avoid legal and highly technical business terminology whenever possible; and

(F) Avoid explanations that are imprecise and readily subject to different interpretations.

(ii) *Designed to call attention.* You design your notice to call attention to the nature and significance of the information in it if you:

(A) Use a plain-language heading to call attention to the notice;

(B) Use a typeface and type size that are easy to read;

(C) Provide wide margins and ample line spacing;

(D) Use boldface or italics for key words; and

(E) In a form that combines your notice with other information, use distinctive type size, style, and graphic devices, such as shading or sidebars, when you combine your notice with other information.

(iii) *Notices on web sites.* If you provide a notice on a web page, you design your notice to call attention to the nature and significance of the information in it if you use text or visual cues to encourage scrolling down the page if necessary to view the entire notice and ensure that other elements on the web site (such as text, graphics, hyperlinks, or sound) do not distract attention from the notice, and you either:

(A) Place the notice on a screen that consumers frequently access, such as a page on which transactions are conducted; or

(B) Place a link on a screen that consumers frequently access, such as a page on which transactions are conducted, that connects directly to the notice and is labeled appropriately to convey the importance, nature and relevance of the notice.

(c) *Collect* means to obtain information that you organize or can retrieve by the name of an individual or by identifying number, symbol, or other identifying particular assigned to the individual, irrespective of the source of the underlying information.

(d) *Company* means any corporation, limited liability company, business trust, general or limited partnership, association, or similar organization.

(e)(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) *Examples*—(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.

(f) *Consumer reporting agency* has the same meaning as in section 603(f) of the Fair Credit Reporting Act (15 U.S.C. 1681a(f)).

(g) *Control* of a company means:

(1) Ownership, control, or power to vote 25 percent or more of the outstanding shares of any class of voting security of the company, directly or indirectly, or acting through one or more other persons;

(2) Control in any manner over the election of a majority of the directors, trustees, or general partners (or individuals exercising similar functions) of the company; or

(3) The power to exercise, directly or indirectly, a controlling influence over the management or policies of the company.

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

(i)(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) *Examples*—(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.

(j) *Federal functional regulator* means:

(1) The Board of Governors of the Federal Reserve System;

(2) The Office of the Comptroller of the Currency;

(3) The Board of Directors of the Federal Deposit Insurance Corporation;

(4) The Director of the Office of Thrift Supervision;

(5) The National Credit Union Administration Board; and

(6) The Securities and Exchange Commission.

(k)(1) *Financial institution* means any institution the business of which is engaging in 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 is a financial institution.

(2) *Examples of financial institution.* (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 and issuing that extension of credit through a proprietary credit card demonstrates that a retailer is significantly engaged in extending credit.

(ii) 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.

(iii) 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.

(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.

(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.

(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 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.

(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.

(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 211.5(d)(15) and referenced in section 4(k)(4)(G) of the Bank Holding Company Act.

(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.

(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.

(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.

(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.*); or

(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 of this part.

(iv) Entities that engage in financial activities but that are not significantly engaged in those financial activities.

(4) *Examples of entities that are not significantly engaged in financial activities.* (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.

(l)(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.

(m)(1) *Nonaffiliated third party* means any person except:

(i) Your affiliate; or

(ii) A person employed jointly by you and any company that is not your affiliate (but *nonaffiliated third party* includes the other company that jointly employs the person).

(2) *Nonaffiliated third party* includes any company that is an affiliate by virtue of your or your affiliate's direct or indirect ownership or control of the company in conducting merchant banking or investment banking activities of the type described in section 4(k)(4)(H) or insurance company investment activities of the type described in section 4(k)(4)(I) of the Bank Holding Company Act (12 U.S.C. 1843(k)(4)(H) and (I)).

(n)(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 (n)(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) *Examples of lists*—(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.

(o)(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) *Examples*—(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.

(p)(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) *Reasonable basis.* 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) *Examples*—(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 web site that is available to the general public on an unrestricted basis. A web site 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.

(q) *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.

Subpart A—Privacy and Opt Out Notices

§ 313.4 Initial privacy notice to consumers required.

(a) *Initial notice requirement.* You must provide a clear and conspicuous notice that accurately reflects your privacy policies and practices to:

(1) *Customer.* An individual who becomes your customer, not later than when you establish a customer relationship, except as provided in paragraph (e) of this section; and

(2) *Consumer.* A consumer, before you disclose any nonpublic personal information about the consumer to any nonaffiliated third party, if you make such a disclosure other than as authorized by §§ 313.14 and 313.15.

(b) *When initial notice to a consumer is not required.* You are not required to provide an initial notice to a consumer under paragraph (a) of this section if:

(1) You do not disclose any nonpublic personal information about the consumer to any nonaffiliated third party, other than as authorized by §§ 313.14 and 313.15; and

(2) You do not have a customer relationship with the consumer.

(c) *When you establish a customer relationship*—(1) *General rule.* You establish a customer relationship when you and the consumer enter into a continuing relationship.

(2) *Special rule for loans.* You establish a customer relationship with a consumer when you originate a loan to the consumer for personal, family, or household purposes. If you subsequently transfer the servicing rights to that loan to another financial institution, the customer relationship transfers with the servicing rights.

(3)(i) *Examples of establishing customer relationship.* You establish a customer relationship when the consumer:

(A) Opens a credit card account with you;

(B) Executes the contract to obtain credit from you or purchase insurance from you;

(C) Agrees to obtain financial, economic, or investment advisory services from you for a fee; or

(D) Becomes your client for the purpose of your providing credit counseling or tax preparation services, or to obtain 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 company or financial institution);

(E) Provides any personally identifiable financial information to you in an effort to obtain a mortgage loan through you;

(F) Executes the lease for personal property with you;

(G) Is an obligor on an account that you purchased from another financial institution and whom you have located and begun attempting to collect amounts owed on the account; or

(H) Provides you with the information necessary for you to compile and provide access to all of the consumer's on-line financial accounts at your Web site.

(ii) *Examples of loan rule.* You establish a customer relationship with a consumer who obtains a loan for personal, family, or household purposes when you:

(A) Originate the loan to the consumer and retain the servicing rights; or

(B) Purchase the servicing rights to the consumer's loan.

(d) *Existing customers.* When an existing customer obtains a new financial product or service from you that is to be used primarily for personal, family, or household purposes, you satisfy the initial notice requirements of paragraph (a) of this section as follows:

(1) You may provide a revised privacy notice, under § 313.8, that covers the customer's new financial product or service; or

(2) If the initial, revised, or annual notice that you most recently provided to that customer was accurate with respect to the new financial product or service, you do not need to provide a new privacy notice under paragraph (a) of this section.

(ii) If it shares with nonaffiliated third parties, state, as applicable: ''*Nonaffiliates we share with can include [list categories of companies such as mortgage companies, insurance companies, direct marketing companies, and nonprofit organizations].*''

(3) *Joint Marketing.* As required by §313.13 of this part, where [*joint marketing*] appears, the financial institution must:

(i) If it does not engage in joint marketing, state: ''*[name of financial institution] doesn't jointly market*''; or

(ii) If it shares personal information for joint marketing, state, as applicable: ''*Our joint marketing partners include [list categories of companies such as credit card companies].*''

(c) *General instructions for the ''Other important information'' box.* This box is optional. The space provided for information in this box is not limited. Only the following types of information can appear in this box.

(1) State and/or international privacy law information; and/or

(2) Acknowledgment of receipt form.

[74 FR 62966, Dec. 1, 2009]

PART 314—STANDARDS FOR SAFEGUARDING CUSTOMER INFORMATION

Sec.

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

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

§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. This part refers to such entities 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.

§314.2 Definitions.

(a) *In general.* Except as modified by this part or unless the context otherwise requires, the terms used in this part have the same meaning as set forth in the Commission's rule governing the Privacy of Consumer Financial Information, 16 CFR part 313.

(b) *Customer information* means any record containing nonpublic personal information as defined in 16 CFR 313.3(n), 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.

(c) *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.

(d) *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.

§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. Such safeguards 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;

West's F.S.A. § 501.171

501.171. Security of confidential personal information

Effective: October 1, 2019

(1) Definitions.--As used in this section, the term:

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

(b) "Covered entity" means a sole proprietorship, partnership, corporation, trust, estate, cooperative, association, or other commercial entity that acquires, maintains, stores, or uses personal information. For purposes of the notice requirements in subsections (3)-(6), the term includes a governmental entity.

(c) "Customer records" means any material, regardless of the physical form, on which personal information is recorded or preserved by any means, including, but not limited to, written or spoken words, graphically depicted, printed, or electromagnetically transmitted that are provided by an individual in this state to a covered entity for the purpose of purchasing or leasing a product or obtaining a service.

(d) "Data in electronic form" means any data stored electronically or digitally on any computer system or other database and includes recordable tapes and other mass storage devices.

(e) "Department" means the Department of Legal Affairs.

(f) "Governmental entity" means any department, division, bureau, commission, regional planning agency, board, district, authority, agency, or other instrumentality of this state that acquires, maintains, stores, or uses data in electronic form containing personal information.

(g)

1. "Personal information" means either of the following:

   a. An individual's first name or first initial and last name in combination with any one or more of the following data elements for that individual:

      (I) A social security number;

      (II) A driver license or identification card number, passport number, military identification number, or other similar number issued on a government document used to verify identity;

      (III) 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;

      (IV) Any information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional; or

      (V) An individual's health insurance policy number or subscriber identification number and any unique identifier used by a health insurer to identify the individual.

   b. 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.

2. The term does not include information about an individual that has been made publicly available by a federal, state, or local governmental entity. The term also does not include information that is encrypted, secured, or modified by any other method or technology that removes elements that personally identify an individual or that otherwise renders the information unusable.

(h) "Third-party agent" means an entity that has been contracted to maintain, store, or process personal information on behalf of a covered entity or governmental entity.

(2) Requirements for data security.--Each covered entity, governmental entity, or third-party agent shall take reasonable measures to protect and secure data in electronic form containing personal information.

(3) Notice to department of security breach.--

(a) A covered entity shall provide notice to the department of any breach of security affecting 500 or more individuals in this state. Such notice must be provided to the department as expeditiously as practicable, but no later than 30 days after the determination of the breach or reason to believe a breach occurred. A covered entity may receive 15 additional days to provide notice as required in subsection (4) if good cause for delay is provided in writing to the department within 30 days after determination of the breach or reason to believe a breach occurred.

(b) The written notice to the department must include:

1. A synopsis of the events surrounding the breach at the time notice is provided.

2. The number of individuals in this state who were or potentially have been affected by the breach.

3. Any services related to the breach being offered or scheduled to be offered, without charge, by the covered entity to individuals, and instructions as to how to use such services.

4. A copy of the notice required under subsection (4) or an explanation of the other actions taken pursuant to subsection (4).

5. The name, address, telephone number, and e-mail address of the employee or agent of the covered entity from whom additional information may be obtained about the breach.

(c) The covered entity must provide the following information to the department upon its request:

1. A police report, incident report, or computer forensics report.

2. A copy of the policies in place regarding breaches.

3. Steps that have been taken to rectify the breach.

(d) A covered entity may provide the department with supplemental information regarding a breach at any time.

(e) For a covered entity that is the judicial branch, the Executive Office of the Governor, the Department of Financial Services, or the Department of Agriculture and Consumer Services, in lieu of providing the written notice to the department, the covered entity may post the information described in subparagraphs (b)1.-4. on an agency-managed website.

(4) Notice to individuals of security breach.--

(a) A covered entity shall give notice to each individual in this state whose personal information was, or the covered entity reasonably believes to have been, accessed as a result of the breach. Notice to individuals shall be made as expeditiously as practicable and without unreasonable delay, taking into account the time necessary to allow the covered entity to determine the scope of the breach of security, to identify individuals affected by the breach, and to restore the reasonable integrity of the data system that was

breached, but no later than 30 days after the determination of a breach or reason to believe a breach occurred unless subject to a delay authorized under paragraph (b) or waiver under paragraph (c).

(b) If a federal, state, or local law enforcement agency determines that notice to individuals required under this subsection would interfere with a criminal investigation, the notice shall be delayed upon the written request of the law enforcement agency for a specified period that the law enforcement agency determines is reasonably necessary. A law enforcement agency may, by a subsequent written request, revoke such delay as of a specified date or extend the period set forth in the original request made under this paragraph to a specified date if further delay is necessary.

(c) Notwithstanding paragraph (a), notice to the affected individuals is not required if, after an appropriate investigation and consultation with relevant federal, state, or local law enforcement agencies, the covered entity reasonably determines that the breach has not and will not likely result in identity theft or any other financial harm to the individuals whose personal information has been accessed. Such a determination must be documented in writing and maintained for at least 5 years. The covered entity shall provide the written determination to the department within 30 days after the determination.

(d) The notice to an affected individual shall be by one of the following methods:

1. Written notice sent to the mailing address of the individual in the records of the covered entity; or

2. E-mail notice sent to the e-mail address of the individual in the records of the covered entity.

(e) The notice to an individual with respect to a breach of security shall include, at a minimum:

1. The date, estimated date, or estimated date range of the breach of security.

2. A description of the personal information that was accessed or reasonably believed to have been accessed as a part of the breach of security.

3. Information that the individual can use to contact the covered entity to inquire about the breach of security and the personal information that the covered entity maintained about the individual.

(f) A covered entity required to provide notice to an individual may provide substitute notice in lieu of direct notice if such direct notice is not feasible because the cost of providing notice would exceed $250,000, because the affected individuals exceed 500,000 persons, or because the covered entity does not have an e-mail address or mailing address for the affected individuals. Such substitute notice shall include the following:

1. A conspicuous notice on the Internet website of the covered entity if the covered entity maintains a website; and

2. Notice in print and to broadcast media, including major media in urban and rural areas where the affected individuals reside.

(g) Notice provided pursuant to rules, regulations, procedures, or guidelines established by the covered entity's primary or functional federal regulator is deemed to be in compliance with the notice requirement in this subsection if the covered entity notifies affected individuals in accordance with the rules, regulations, procedures, or guidelines established by the primary or functional federal regulator in the event of a breach of security. Under this paragraph, a covered entity that timely provides a copy of such notice to the department is deemed to be in compliance with the notice requirement in subsection (3).

(5) Notice to credit reporting agencies.--If a covered entity discovers circumstances requiring notice pursuant to this section of more than 1,000 individuals at a single time, the covered entity shall also notify, without unreasonable delay, all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined in the Fair Credit Reporting Act, 15 U.S.C. s. 1681a(p), of the timing, distribution, and content of the notices.

(6) Notice by third-party agents; duties of third-party agents; notice by agents.--

(a) In the event of a breach of security of a system maintained by a third-party agent, such third-party agent shall notify the covered entity of the breach of security as expeditiously as practicable, but no later than 10 days following the determination of the breach of security or reason to believe the breach occurred. Upon receiving notice from a third-party agent, a covered entity shall provide notices required under subsections (3) and (4). A third-party agent shall provide a covered entity with all information that the covered entity needs to comply with its notice requirements.

(b) An agent may provide notice as required under subsections (3) and (4) on behalf of the covered entity; however, an agent's failure to provide proper notice shall be deemed a violation of this section against the covered entity.

(7) Annual report.--By February 1 of each year, the department shall submit a report to the President of the Senate and the Speaker of the House of Representatives describing the nature of any reported breaches of security by governmental entities or third-party agents of governmental entities in the preceding calendar year along with recommendations for security improvements. The report shall identify any governmental entity that has violated any of the applicable requirements in subsections (2)-(6) in the preceding calendar year.

(8) Requirements for disposal of customer records.--Each covered entity or third-party agent shall take all reasonable measures to dispose, or arrange for the disposal, of customer records containing personal information within its custody or control when the records are no longer to be retained. Such disposal shall involve shredding, erasing, or otherwise modifying the personal information in the records to make it unreadable or undecipherable through any means.

(9) Enforcement.--

(a) A violation of this section shall be treated as an unfair or deceptive trade practice in any action brought by the department under s. 501.207 against a covered entity or third-party agent.

(b) In addition to the remedies provided for in paragraph (a), a covered entity that violates subsection (3) or subsection (4) shall be liable for a civil penalty not to exceed $500,000, as follows:

1. In the amount of $1,000 for each day up to the first 30 days following any violation of subsection (3) or subsection (4) and, thereafter, $50,000 for each subsequent 30-day period or portion thereof for up to 180 days.

2. If the violation continues for more than 180 days, in an amount not to exceed $500,000.

The civil penalties for failure to notify provided in this paragraph apply per breach and not per individual affected by the breach.

(c) All penalties collected pursuant to this subsection shall be deposited into the General Revenue Fund.

(10) No private cause of action.--This section does not establish a private cause of action.

(11) Public records exemption.--

(a) All information received by the department pursuant to a notification required by this section, or received by the department pursuant to an investigation by the department or a law enforcement agency, is confidential and exempt from s. 119.07(1) and s. 24(a), Art. I of the State Constitution, until such time as the investigation is completed or ceases to be active. This exemption shall be construed in conformity with s. 119.071(2)(c).

(b) During an active investigation, information made confidential and exempt pursuant to paragraph (a) may be disclosed by the department:

1. In the furtherance of its official duties and responsibilities;

2. For print, publication, or broadcast if the department determines that such release would assist in notifying the public or locating or identifying a person that the department believes to be a victim of a data breach or improper disposal of customer records, except that information made confidential and exempt by paragraph (c) may not be released pursuant to this subparagraph; or

3. To another governmental entity in the furtherance of its official duties and responsibilities.

(c) Upon completion of an investigation or once an investigation ceases to be active, the following information received by the department shall remain confidential and exempt from s. 119.07(1) and s. 24(a), Art. I of the State Constitution:

1. All information to which another public records exemption applies.

2. Personal information.

3. A computer forensic report.

4. Information that would otherwise reveal weaknesses in a covered entity's data security.

5. Information that would disclose a covered entity's proprietary information.

(d) For purposes of this subsection, the term "proprietary information" means information that:

1. Is owned or controlled by the covered entity.

2. Is intended to be private and is treated by the covered entity as private because disclosure would harm the covered entity or its business operations.

3. Has not been disclosed except as required by law or a private agreement that provides that the information will not be released to the public.

4. Is not publicly available or otherwise readily ascertainable through proper means from another source in the same configuration as received by the department.

5. Includes:

a. Trade secrets as defined in s. 688.002.

b. Competitive interests, the disclosure of which would impair the competitive business of the covered entity who is the subject of the information.

Credits

Added by Laws 2014, c. 2014-189, § 3, eff. July 1, 2014. Amended by Laws 2014, c. 2014-190, § 1, eff. July 1, 2014; Laws 2019, c. 2019-32, § 1, eff. Oct. 1, 2019.

West's F. S. A. § 501.171, FL ST § 501.171
Current with chapters from the 2020 Second Regular Session of the 26th Legislature in effect through July 01, 2020

End of Document

16 C.F.R. § 682.1

§ 682.1 Definitions.

Effective: June 1, 2005

(a) In general. Except as modified by this part or unless the context otherwise requires, the terms used in this part have the same meaning as set forth in the Fair Credit Reporting Act, 15 U.S.C. 1681 et seq.

(b) "Consumer information" means any record about an individual, whether in paper, electronic, or other form, that is a consumer report or is derived from a consumer report. Consumer information also means a compilation of such records. Consumer information does not include information that does not identify individuals, such as aggregate information or blind data.

(c) "Dispose," "disposing," or "disposal" means:

(1) The discarding or abandonment of consumer information, or

(2) The sale, donation, or transfer of any medium, including computer equipment, upon which consumer information is stored.

SOURCE: 69 FR 35496, June 24, 2004; 69 FR 68697, Nov. 24, 2004; 84 FR 31191, July 1, 2019, unless otherwise noted.

AUTHORITY: Pub.L. 108–159, sec. 216.

Current through July 30, 2020, 85 FR 45808.

End of Document

16 C.F.R. § 682.2

§ 682.2 Purpose and scope.

Effective: June 1, 2005

Currentness

(a) Purpose. This part ("rule") implements section 216 of the Fair and Accurate Credit Transactions Act of 2003, which is designed to reduce the risk of consumer fraud and related harms, including identity theft, created by improper disposal of consumer information.

(b) Scope. This rule applies to any person over which the Federal Trade Commission has jurisdiction, that, for a business purpose, maintains or otherwise possesses consumer information.

SOURCE: 69 FR 35496, June 24, 2004; 69 FR 68697, Nov. 24, 2004; 84 FR 31191, July 1, 2019, unless otherwise noted.

AUTHORITY: Pub.L. 108–159, sec. 216.

Current through July 30, 2020, 85 FR 45808.

End of Document

16 C.F.R. § 682.3

§ 682.3 Proper disposal of consumer information.

Effective: June 1, 2005

Currentness

(a) Standard. Any person who maintains or otherwise possesses consumer information for a business purpose must properly dispose of such information by taking reasonable measures to protect against unauthorized access to or use of the information in connection with its disposal.

(b) Examples. Reasonable measures to protect against unauthorized access to or use of consumer information in connection with its disposal include the following examples. These examples are illustrative only and are not exclusive or exhaustive methods for complying with the rule in this part.

(1) Implementing and monitoring compliance with policies and procedures that require the burning, pulverizing, or shredding of papers containing consumer information so that the information cannot practicably be read or reconstructed.

(2) Implementing and monitoring compliance with policies and procedures that require the destruction or erasure of electronic media containing consumer information so that the information cannot practicably be read or reconstructed.

(3) After due diligence, entering into and monitoring compliance with a contract with another party engaged in the business of record destruction to dispose of material, specifically identified as consumer information, in a manner consistent with this rule. In this context, due diligence could include reviewing an independent audit of the disposal company's operations and/or its compliance with this rule, obtaining information about the disposal company from several references or other reliable sources, requiring that the disposal company be certified by a recognized trade association or similar third party, reviewing and evaluating the disposal company's information security policies or procedures, or taking other appropriate measures to determine the competency and integrity of the potential disposal company.

(4) For persons or entities who maintain or otherwise possess consumer information through their provision of services directly to a person subject to this part, implementing and monitoring compliance with policies and procedures that protect against unauthorized or unintentional disposal of consumer information, and disposing of such information in accordance with examples (b)(1) and (2) of this section.

(5) For persons subject to the Gramm–Leach–Bliley Act, 15 U.S.C. 6081 et seq., and the Federal Trade Commission's

Standards for Safeguarding Customer Information, 16 CFR part 314 ("Safeguards Rule"), incorporating the proper disposal of consumer information as required by this rule into the information security program required by the Safeguards Rule.

SOURCE: 69 FR 35496, June 24, 2004; 69 FR 68697, Nov. 24, 2004; 84 FR 31191, July 1, 2019, unless otherwise noted.

AUTHORITY: Pub.L. 108–159, sec. 216.

Notes of Decisions (2)

Current through July 30, 2020, 85 FR 45808.

End of Document

16 C.F.R. § 682.4

§ 682.4 Relation to other laws.

Effective: June 1, 2005

Currentness

Nothing in the rule in this part shall be construed:

(a) To require a person to maintain or destroy any record pertaining to a consumer that is not imposed under other law; or

(b) To alter or affect any requirement imposed under any other provision of law to maintain or destroy such a record.

SOURCE: 69 FR 35496, June 24, 2004; 69 FR 68697, Nov. 24, 2004; 84 FR 31191, July 1, 2019, unless otherwise noted.

AUTHORITY: Pub.L. 108–159, sec. 216.

Current through July 30, 2020, 85 FR 45808.

16 C.F.R. § 682.5

§ 682.5 Effective date.

Effective: June 1, 2005

Currentness

The rule in this part is effective on June 1, 2005.

SOURCE: 69 FR 35496, June 24, 2004; 69 FR 68697, Nov. 24, 2004; 84 FR 31191, July 1, 2019, unless otherwise noted.

AUTHORITY: Pub.L. 108–159, sec. 216.

Current through July 30, 2020, 85 FR 45808.

West's F.S.A. Bar Rule 4-1.6

Rule 4-1.6. Confidentiality of Information

Currentness

(a) Consent Required to Reveal Information. A lawyer must not reveal information relating to representation of a client 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:

(1) to prevent a client from committing a crime; or

(2) to prevent a death or substantial bodily harm to another.

(c) When Lawyer May Reveal Information. A lawyer may reveal confidential information to the extent the lawyer reasonably believes necessary:

(1) to serve the client's interest unless it is information the client specifically requires not to be disclosed;

(2) to establish a claim or defense on behalf of the lawyer in a controversy between the lawyer and client;

(3) to establish a defense to a criminal charge or civil claim against the lawyer based on conduct in which the client was involved;

(4) to respond to allegations in any proceeding concerning the lawyer's representation of the client;

(5) to comply with the Rules Regulating The Florida Bar; or

(6) to 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 attorney-client privilege or otherwise prejudice the client.

(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 representation of a client.

(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.

Credits

Amended July 23, 1992, effective Jan. 1, 1993 (605 So.2d 252); Oct. 20, 1994 (644 So.2d 282); March. 23, 2006, effective May 22, 2006 (933 So.2d 417); May 29, 2014, effective June 1, 2014 (140 So.3d 541); June 11, 2015, effective Oct. 1, 2015 (167 So.3d 412).

Editors' Notes

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.

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.

Notes of Decisions (63)

West's F. S. A. Bar Rule 4-1.6, FL ST BAR Rule 4-1.6
Florida Supreme Court Rules of Civil Procedure, Judicial Administration, Criminal Procedure, Civil Procedure for Involuntary Commitment of Sexually Violent Predators, Worker's Compensation, Probate, Traffic Court, Small Claims, Juvenile Procedure, Appellate Procedure, Certified and Court-Appointed Mediators, Court Appointed Arbitrators, Family Law, Certification and Regulation of Court Reporters, Certification of Spoken Language Interpreters, and Qualified and Court-Appointing Parenting Coordinators are current with amendments received through 2/15/20. All other State Court Rules are current with amendments received through 6/15/20.

End of Document

Avoid Being Hacked: Perform a Network Penetration Test

August 4, 2020

The **FBI** and **FinCEN** have issued advisories warning of increased cyberattacks aimed at stealing money, personal information or both. Want to protect your computer network from being hacked? Experts say companies should perform what's called a "Penetration Test" to find any vulnerabilities in your network.

"A penetration test simulates an attacker attacking a network. The goal of a penetration test is to identify real-world vulnerabilities that would be valuable to an attacker," explained Alex Lauerman, founder and principal consultant at TrustFoundry, an internet security firm based in Overland Park, Kan.

In effect, when you perform a penetration test, you pay a company to try to hack your system, find inroads and repair them before hackers can exploit them.

"Penetration testing identifies many vulnerabilities before attackers do," Lauerman said. "Unfortunately, it is easy to make small configuration or technical mistakes (when setting up a computer network) that can put large amounts of sensitive information at risk. These mistakes can be difficult to identify, although attackers are experts at finding and exploiting them. An attacker only has to win once, especially on an internet-facing server."

Recently, Punctual Abstract, a real estate title abstracting firm headquartered in Harvey, La., hired TrustFoundry to perform a penetration test on its external network.

"When our customers order title evidence from Punctual Abstract, they trust that we will provide accurate information," said Punctual Abstract CEO Ted Woloszyk. "Our responsibilities don't end there. We need to make sure our title evidence is held in a secure manner and that we do not leave that information vulnerable for someone to steal it. Even though the information we gather is public record, it is sensitive when you bring it all together and put it in one spot."

Punctual Abstract's proprietary software integrates with several of the industry's settlement services platforms, allowing title agencies to automate the creation of real estate closing documents utilizing property research conducted by Punctual Abstract. This information is transmitted over the internet, which is another reason why network security is crucial. Hence, the penetration test.

"It's all about trust and integrity. We want our customers to know we're doing the right thing even when no one is looking," Woloszyk says. "Our customers don't want to be doing business with companies who don't have proper control of their data."

Lauerman says when companies go shopping for network security tests, it's important to know what you're buying. There is a difference between a vulnerability assessment and a penetration test. He explains that a vulnerability assessment is primarily an automated assessment, which combines the information from multiple tools and is validated to remove false positives. Penetration testing digs much deeper to find and exploit vulnerabilities, such as weak credentials, advanced web application

issues, and exposed assets and information in various places that the company may not know about.

“Penetration testing is an important part of a security program,” Lauerman said. “A company that conducts penetration testing is more likely to keep their customer’s data secure. Penetration testing is an increasingly common requirement for companies, driven both by their customers and also internal pressure to uphold and maintain data security.”

Most frequently, penetration testing is performed once a year, although it’s up to the company to determine what is warranted. The industry is moving towards more continuous testing to help identify any changes that may occur throughout the year.

For most companies with a moderate amount of public-facing infrastructure, the cost of external network penetration testing is between $5,000 and $15,000.

Punctual Abstract’s IT staff was able to make several changes and improvements as a result of TrustFoundry’s penetration test.

Woloszyk says those fixes help him to have peace of mind. Yet, the company remains vigilant by training staff in practices that protect Punctual Abstract’s data integrity. “It’s an ongoing process,” he said.

FEDERAL TRADE COMMISSION
PROTECTING AMERICA'S CONSUMERS

SMALL BUSINESS COMPUTER SECURITY BASICS

TAGS: Privacy and Security | Data Security | Appliances | Automobiles | Clothing and Textiles | Franchises, Business Opportunities, and Investments | Human Resources | Jewelry | Non-Profits | spyware and malware

If you're running a small business with only a few employees, you've learned about a lot of things – accounting, marketing, HR, you name it. And you probably depend on technology, even if it's only a computer and a phone. You can't afford to get thrown off-track by a hacker or scammer.

Here are a few computer security basics to help your company, even if you're the only employee. If you have employees, train them to follow these tips. If you collect any consumer information, also check out our advice about protecting personal information.

PROTECT YOUR FILES & DEVICES

Keep your software up-to-date. No matter what operating system, browser or other software you use, keep it up to date. Set it to update automatically so you don't leave holes hackers can exploit.

Back up your files. No system is completely secure. Create offline backups of important files. That way, if your computer is compromised, you'll still have access to your files.

Use strong passwords. The longer the better – at least 12 characters. Complexity also helps strengthen a password. Mix numbers, symbols, and capital letters into the middle of the password, not at the beginning or end. Don't use patterns to lengthen a password. Never use the same password for more than one account, or for personal and business accounts. If you write them down, lock them up. Consider using a password manager, an easy-to-access application that allows you to store all your valuable password information in one place. Be sure to protect your password manager with a strong master password, and only use a password manager from a reputable company. Don't share passwords on the phone, in texts or by email.

Turn on two-factor authentication. For accounts that support it, two-factor authentication requires both your password and an additional piece of information to log in to your account. The second piece could be a code sent to your phone, or a random number generated by an app or a token. This protects your account even if your password is compromised.

Don't leave your laptop, phone or other devices unattended in public, even locked in a car. They may contain sensitive information – and they're costly to replace. If they go missing, the information stored on them may fall into the

hands of an identity thief. You also can turn on device encryption to encrypt all data on each device. This reduces the risk to sensitive information in case your device is stolen or misplaced.

Password protect all your devices. If you access your business network from an app on your phone or tablet, use a strong password for the app, too.

THINK BEFORE YOU SHARE YOUR INFORMATION

Protect account information. *Every time* someone asks for business information – whether in an email, text, phone call or web form – think about whether you can really trust the request. Scammers will say or do anything – or pretend to be anyone – to get account numbers, credit card numbers, Social Security numbers or other credentials. Scammers will rush, pressure or threaten you to get you to give up company information.

Only give sensitive information over encrypted websites. If your company is banking or buying online, stick to sites that use encryption to protect your information as it travels from your computer to their server. Look for **https** at the beginning of the web address in the address bar of your browser. Look for https on every page of the site you're on, not just where you log in.

PROTECT YOUR WIRELESS NETWORK

Set up your router securely. If your small business has a wireless network, your "access point" is probably a cable or DSL modem connected to a wireless router, which sends a signal through the air. Your router directs traffic between your local network and the internet. Any device within range can pull the signal from the air and access the internet. If you don't secure your router, strangers could easily gain access to sensitive personal or financial information on your devices.

> ***Change the name of your router from the default.*** The name of your router (often called the service set identifier or SSID) is likely to be a standard, default ID assigned by the manufacturer. Change the name to something unique that only you know. Visit the company's website to learn how to change the router name.
>
> ***Change your router's pre-set password(s).*** Hackers know the default passwords, so change yours to something only you know. The same goes for any default "user" passwords. Use long and complex passwords. Visit the company's website to learn how to change the password.
>
> ***Keep your router's software up to date***. Before you set up a new router, and periodically thereafter, visit the manufacturer's website to see if there's a new version of the software available for download. To make sure you hear about the latest version, register your router with the manufacturer and sign up to get updates.
>
> ***Turn off any "remote management" features.*** Some routers offer an option to allow remote access to your router's controls, such as enabling the manufacturer to provide technical support. Never leave this feature enabled. Hackers can use them to get into your network.
>
> ***Log out as administrator.*** Once you've set up your router, log out as administrator, to lessen the risk that someone can piggyback on your session to gain control of your device.

Use encryption on your wireless network. Encrypt the information you send over your wireless network, so that nearby attackers can't understand your communications. Encryption scrambles the information you send into a code so that it's not accessible to others. Modern routers offer WPA2, the strongest wireless encryption widely available. To protect your data, use it.

Wireless routers often come with the encryption feature turned off. You must turn it on. The directions that come with your router should explain how. If they don't, check the company's website.

Limit access to your network. Allow only specific devices to access your wireless network. Wireless routers usually have a mechanism to allow only devices with particular unique Media Access Control (MAC) address to access to the network. If you want to provide free Wi-Fi for your customers, set up a second, public network – separate from the network for your business devices.

BE CAREFUL WITH WI-FI HOTSPOTS

If you're on the go, Wi-Fi hotspots in coffee shops, libraries, airports, hotels, and other public places are convenient – but often they're not secure. In fact, if a network doesn't require a WPA2 password, it's probably not secure. To protect your information when using wireless hotspots, send information only to websites that are fully encrypted – look for **https** on every page. And avoid using mobile apps that require sharing personal or financial information over public Wi-Fi.

KNOW WHAT TO DO IF SOMETHING GOES WRONG

Plan ahead so you know what to do if a hacker gets into your system. There are steps you can take to minimize the damage if you discover malware on your computers, that your email has been hacked, or even if someone takes over your system and demands a ransom to return control of it.

And if someone accesses personal or financial information that they shouldn't, take steps to respond to that data breach.

spyware and malware
April 2017

ftc.gov

ALTA Rapid Response Plan for Wire Fraud Incidents

https://www.alta.org/file.cfm?name=ALTA-Rapid-Response-Plan-for-Wire-Fraud-Incidents

Time is of the essence – every second and minute counts.
Contact banks, transaction parties, and law enforcement immediately upon discovery.

Step 1: Alert company management and your internal wire fraud response team.

Contact your team according to a pre-arranged plan (group email; group text):

- Owner / Manager
- Accounting / Finance / Treasurer
- IT / IT Security
- Legal Counsel
- Others?

Step 2: Report Fraudulent Wire Transfers to the Sending and Receiving Banks.

- Contact the sending bank's fraud department and request that a recall of the wire be sent to the receiving bank because of fraud. Provide the details for the wire.
- Ask the sending bank to initiate the FBI's Financial Fraud Kill Chain if the amount of the wire transfer is $50,000 or above; the wire transfer is international; a SWIFT recall notice has been initiated; and the wire transfer has occurred within the last 72 hours.
- Also call the receiving bank's fraud department to notify them that you have requested a recall of the wire because of fraud. Provide the details for the wire and request that the account be frozen.
- If a client or consumer was a victim and your bank/accounts were not directly involved, your client or customer will need to contact the bank themselves but you may have helpful information to share, too. Coordinate quickly!

Step 3: Report Fraudulent Wire Transfers and Attempts to Law Enforcement.

- Local Police/Sheriff: https://www.policeone.com/law-enforcement-directory/
- FBI Field Office: https://www.fbi.gov/contact-us/field-offices
- Secret Service: https://www.secretservice.gov/contact/field-offices/

Step 4: Call the sending bank again to confirm that the recall request has been processed.

Step 5: Inform the parties to the transaction (buyer, seller, real estate agents, broker, attorneys, underwriter, notary, etc.) using known, trusted, phone numbers for verbal verification.

If you're unsure about what to say, here's a sample: "There appears to have been [attempted] wire fraud associated with this transaction. We recommend that you review your email security and update passwords and take any other appropriate security measures immediately. For the remainder of this transaction, all communication will occur using known, trusted, telephone numbers."

Step 6: Review your Incident Response Plan to determine if you need to update passwords, secure hardware, and review email logs to determine how and when email accounts were accessed.

Step 7: Consider contacting your insurance carrier(s) and outside legal counsel.

Step 8: If funds were wired out of the U.S., hire an attorney in that country to help recover funds.

Step 9: Document your response using a Response Worksheet.

- Customize this ALTA Rapid Response Plan for Wire Fraud Incidents
- Customize a Response Worksheet (available in Excel or PDF)
- Assign each step to an appropriate person/entity
- Track progress through to completion or resolution
- Retain the Response Worksheet for future reference/update

Step 10: File a complaint with the FBI's Internet Crime Complaint Center (IC3).

Visit www.ic3.gov and provide the following information:

- Victim's name, address, telephone, and email
- Financial transaction information (e.g., account information, transaction date and amount, who received the money)
- Subject's name, address, telephone, email, website, and IP address
- Specific details on how you were victimized
- For Business Email Compromise (BEC) events, copy email header(s) – Learn how
- Any other relevant information that is necessary to support the claimant

ALTA Outgoing Wire Preparation Checklist

Date: _____

File Number: _____

Company Name/Location: _____

Section 1:
Provide the source of the wiring instructions:

☐ I received the initial outgoing wire instructions directly from the **payee in person**. The instructions have not been modified or amended. **Proceed to Section 2.**

☐ I received the initial outgoing wire instructions directly from the **payee via the United States Postal Service or a known overnight mail or messenger service** and **verified** the accuracy of the instruction by **calling the payee** at a phone number obtained independently from any phone number shown in the package. The instructions have not been modified or amended. **Proceed to Section 2.**

☐ I received the initial outgoing wire instructions directly from the **payee via fax** and **verified** the accuracy of the instruction by **calling the payee** at a phone number obtained independently from any phone number shown in the package. The instructions have not been modified or amended. **Proceed to Section 2.**

☐ I received the initial outgoing wire instructions from the **payee**, which have been modified or amended in writing in person at the following date/time: _____. **Proceed to Section 2.**

☐ I received the initial outgoing wire instructions directly from the **payee by email** and **verified** the accuracy of the instruction by **calling the payee** at a phone number obtained independently from any phone number shown in the email. The instructions have not been modified or amended. **Proceed to Section 2.**

☐ I received the initial outgoing wiring instructions **via a 3rd party** (e.g., attorney, realtor, lender) and have **verified** the accuracy of the instruction by **calling the payee** at a phone number obtained independently from any phone number obtained via the 3rd party. The instructions have not been modified or amended. **Proceed to Section 2.**

Section 2:
Verify instructions received by email or from someone other than the payee.

☐ **Wire Payee Name:** _____

☐ **Wire Amount:** _____

☐ **Payee Phone Number:** _____

☐ **Source of Phone Number**
(never use the phone number included in an email):

- ☐ Original Order or Contract: _____
- ☐ Secure Portal: _____
- ☐ Internet Search: _____
- ☐ Other (describe): _____

☐ **Name of Person I Spoke With:** _____

☐ **Date:** _____

☐ **Wire Information confirmed.** Account and ABA Routing Number, and Account Name match payee in the file. Wire instruction notes indicate correct payment information (e.g., loan number, beneficiary, other information).

☐ **Wire Information confirmed.** Account and ABA Routing Number match an entry on our company's list of validated wire instructions for common bank payoffs.

Wire Creator: _____
(Signature) (Date)

_____
(Printed Name)

Wire Authorizer: _____
(Signature) (Date)

_____
(Printed Name)

ALTA Outgoing Wire Preparation Checklist

Section 3:
Verify Delivery of Wired Funds.

- ☐ Date Wire Was Sent: _____
- ☐ Date Wire Was Received: _____
- ☐ Person Confirming Receipt: _____
- ☐ Purpose of Wire: _____
  - ☐ Loan Payoff _____
  - ☐ Equity Loan Payoff _____
  - ☐ Seller Proceeds _____
  - ☐ Real Estate Commission _____
  - ☐ Other (describe): _____

Verified By: _____
(Signature) (Date)

_____
(Printed Name)

MEMBER AMERICAN LAND TITLE ASSOCIATION

For more information and tools to prevent wire fraud, **visit the ALTA Website:**

alta.org/business-tools/information-security.cfm

Protect Your Practice From Wire Fraud Schemes

Every day, hackers try to steal your money by emailing fake wire instructions. Criminals will use a similar email address and steal a logo and other info to make it look like the email came from a reputable source you know.

Protect yourself and your firm by following these steps:

Be Vigilant

- **Call, don't email:** Confirm your wiring instructions by phone using a known number before transferring funds. Don't use phone numbers or links from an email.
- **Be suspicious:** If anything about the transaction doesn't feel right, STOP!

Protect Your Money

- **Confirm everything:** Ask the bank to confirm all info on the account before any money is sent.
- **Verify immediately:** Within four to eight hours, call and confirm the money was received.

What To Do If You've Been Targeted

- **Immediately call the bank** and ask them to issue a recall notice.
- **Report the crime to IC3.gov**
- **Call your regional FBI office and police.**
- Detecting that you sent money to the wrong account **within 24 hours** is the best chance of recovering your money.

OLD REPUBLIC TITLE

rev. 07/2016

FACTS

WHAT DOES OLD REPUBLIC TITLE DO WITH YOUR PERSONAL INFORMATION?

Why?	Financial companies choose how they share your personal information. Federal law gives consumers the right to limit some but not all sharing. Federal law also requires us to tell you how we collect, share, and protect your personal information. Please read this notice carefully to understand what we do.
What?	The types of personal information we collect and share depend on the product or service you have with us. This information can include: • Social Security number and employment information • Mortgage rates and payments and account balances • Checking account information and wire transfer instructions When you are *no longer* our customer, we continue to share your information as described in this notice.
How?	All financial companies need to share customers' personal information to run their everyday business. In the section below, we list the reasons financial companies can share their customers' personal information; the reasons Old Republic Title chooses to share; and whether you can limit this sharing.

Reasons we can share your personal information	Does Old Republic Title share?	Can you limit this sharing?
For our everyday business purposes — such as to process your transactions, maintain your account(s), or respond to court orders and legal investigations, or report to credit bureaus	**Yes**	**No**
For our marketing purposes — to offer our products and services to you	**No**	**We don't share**
For joint marketing with other financial companies	**No**	**We don't share**
For our affiliates' everyday business purposes — information about your transactions and experiences	**Yes**	**No**
For our affiliates' everyday business purposes — information about your creditworthiness	**No**	**We don't share**
For our affiliates to market to you	**No**	**We don't share**
For non-affiliates to market to you	**No**	**We don't share**

Questions	**Go to** www.oldrepublictitle.com (*Contact Us*)

Who we are	
Who is providing this notice?	Companies with an Old Republic Title name and other affiliates. Please see below for a list of affiliates.

What we do	
How does Old Republic Title protect my personal information?	To protect your personal information from unauthorized access and use, we use security measures that comply with federal law. These measures include computer safeguards and secured files and buildings. For more information, visit http://www.OldRepublicTitle.com/newnational/Contact/privacy.
How does Old Republic Title collect my personal information?	We collect your personal information, for example, when you: • Give us your contact information or show your driver's license • Show your government-issued ID or provide your mortgage information • Make a wire transfer We also collect your personal information from others, such as credit bureaus, affiliates, or other companies.
Why can't I limit all sharing?	Federal law gives you the right to limit only: • Sharing for affiliates' everyday business purposes - information about your creditworthiness • Affiliates from using your information to market to you • Sharing for non-affiliates to market to you State laws and individual companies may give you additional rights to limit sharing. See the "Other important information" section below for your rights under state law.

Definitions	
Affiliates	Companies related by common ownership or control. They can be financial and nonfinancial companies. • *Our affiliates include companies with an Old Republic Title name, and financial companies such as Attorneys' Title Fund Services, LLC, Lex Terrae National Title Services, Inc., Mississippi Valley Title Services Company, and The Title Company of North Carolina.*
Non-affiliates	Companies not related by common ownership or control. They can be financial and non-financial companies. • *Old Republic Title does not share with non-affiliates so they can market to you*
Joint marketing	A formal agreement between non-affiliated financial companies that together market financial products or services to you. • *Old Republic Title doesn't jointly market*.

Other Important Information

Oregon residents only: We are providing you this notice under state law. We may share your personal information (described on page one) obtained from you or others with non-affiliate service providers with whom we contract, such as notaries and delivery services, in order to process your transactions. You may see what personal information we have collected about you in connection with your transaction (other than personal information related to a claim or legal proceeding). To see your information, please click on "Contact Us" at www.oldrepublictitle.com and submit your written request to the Legal Department. You may see and copy the information at our office or ask us to mail you a copy for a reasonable fee. If you think any information is wrong, you may submit a written request online to correct or delete it. We will let you know what actions we take. If you do not agree with our actions, you may send us a statement.

Affiliates Who May be Delivering This Notice

American First Abstract, LLC	**American First Title & Trust Company**	**American Guaranty Title Insurance Company**	**Attorneys' Title Fund Services, LLC**	**Compass Abstract, Inc.**
eRecording Partners Network, LLC	**Genesis Abstract, LLC**	**Kansas City Management Group, LLC**	**L.T. Service Corp.**	**Lenders Inspection Company**
Lex Terrae National Title Services, Inc.	**Lex Terrae, Ltd.**	**Mara Escrow Company**	**Mississippi Valley Title Services Company**	**National Title Agent's Services Company**
Old Republic Branch Information Services, Inc.	**Old Republic Diversified Services, Inc.**	**Old Republic Exchange Company**	**Old Republic National Title Insurance Company**	**Old Republic Title and Escrow of Hawaii, Ltd.**
Old Republic Title Co.	**Old Republic Title Company of Conroe**	**Old Republic Title Company of Indiana**	**Old Republic Title Company of Nevada**	**Old Republic Title Company of Oklahoma**
Old Republic Title Company of Oregon	**Old Republic Title Company of St. Louis**	**Old Republic Title Company of Tennessee**	**Old Republic Title Information Concepts**	**Old Republic Title Insurance Agency, Inc.**
Old Republic Title, Ltd.	**Republic Abstract & Settlement , LLC**	**Sentry Abstract Company**	**The Title Company of North Carolina**	**Title Services, LLC**
Trident Land Transfer Company, LLC				

A PROGRAM OF IBHS

Prepared by the Insurance Institute for Business & Home Safety (IBHS), which is an independent, nonprofit, scientific research and communications organization supported by the property insurance industry. The Institute works to reduce the social and economic effects of natural disasters and other risks on residential and commercial property by conducting building science research and advocating improved construction, maintenance and preparedness practices.

THE EASY WAY TO PREPARE YOUR BUSINESS FOR THE UNEXPECTED.

Insurance Institute for Business & Home Safety®

Contents

Overview

The Insurance Institute for Business & Home Safety (IBHS) has developed a new streamlined business continuity program for small businesses that may not have the time or resources to create an extensive plan to recover from business interruptions. IBHS is a leading national expert on preparing for, and repairing, rebuilding, and recovering from catastrophes both large and small. IBHS' mission is to conduct objective, scientific research to identify and promote effective actions that strengthen homes, businesses, and communities against natural disasters and other causes of loss.

IBHS' original business continuity program is called Open for Business®, or OFB. The new program, OFB-EZ®, is designed to be simple to use, administer and implement. With OFB-EZ, you can follow the same disaster planning and recovery processes used by larger companies – but without a large company budget. OFB-EZ is user-friendly and does not require any previous experience with or knowledge of business continuity planning.

This toolkit will help you:

1. identify the business activities that are essential for continued operation during a disruption;
2. deal with risks your organization faces; and
3. create an easy-to-use recovery plan tailored to your business, giving you confidence if the worst occurs.

Statistics show that one in four businesses forced to close because of a disaster never reopen. Small businesses, which form the backbone of the United States economy, are particularly at risk. IBHS' ultimate goal is for every small business to prepare a plan that will enable them to withstand and recover from any type of disruption.

Know Your Risks

Knowing your risks will help you evaluate the extent of your business' vulnerability to disruptions.

How potential threats impact each business varies considerably because no two businesses are exactly alike. Differences in location, industry, culture, business structure, management style, work functions and business objectives affect how you choose to protect your business from threats and how you respond to and recover from a business disruption.

The two biggest mistakes many small businesses make are failing to identify a potential threat, and underestimating the severity of a known potential threat. After completing the risk assessment, you will be able to determine the greatest threats to your business, the likelihood or probability for each of those threats, how severe each event could be, and the potential impact on each business function or process.

Identify Your Threats.

Use the Vulnerability and Risk Assessment to determine the threats that are likely to affect your business. Add any additional threats you are exposed to that are not already listed.

Rank the Probability of Threats.

How likely is it to happen? Assign a rank of 0 to 5 in the Probability Level row.

Rank the Severity of Threats.

You will need to assess the potential impact of each threat, which means the amount of damage the event is capable of causing. To measure the potential damage, think about the duration, magnitude, and the extent of the potential threat's reach (e.g., just one floor of your building, the entire structure, a neighborhood, the entire region, etc). After assessing all these factors, assign a rank of 0 to 5 in the Severity Level row.

Multiply the Probability and Severity Scores for Each Threat.

Once you have ranked the probability and severity levels for each threat, multiply values and record the total in the Total Value column.

The highest ranking threats (17-25) are those you will need to plan for as soon as possible. You should assume those hazards will strike your business, and determine what controls you have in place or could implement to minimize your risk.

RECOMMENDATIONS:

For a list of natural hazards that may affect your business' location, use the Insurance Institute for Business & Home Safety's (IBHS) ZIP Code tool to identify hazards in your area, and generate a customized list of projects that can reduce your risk.

You also should consider damage to infrastructure (e.g., roads, bridges, electric power, etc.) that could affect your ability to resume operations, and develop possible workarounds to expedite recovery.

In addition, contact your local emergency management office to obtain a copy of your community's hazards vulnerability analysis for a list of possible natural and man-made hazards that could affect your area.

About the Form

You should review and update your Vulnerability and Risk Assessment every six months. You will find that new ideas or considerations will surface each time, helping you refine your thinking and modify your plan. It is important to establish a maintenance program to keep your plan's contents current and relevant.

Know Your Risks

Use this form to review potential threats. Fill in one field for probability and one field for severity. Finally, multiply the probability and severity levels and enter the total in the total value column.

THREATS	Probability (0-5)	Severity (0-5)	Total
Earthquake			
Tornado/Wind/Hurricane			
Flood			
Severe Winter Weather			
Interior Fire			
Wildfire			
Loss/Illness of Key Staff			
Workplace Violence			
Software/Hardware Failure			
Power Outage			
Loss of Utilites (water, gas, electricity, etc.)			
Pandemic/Epidemic/Flu			
Loss of Premises			
Other			
Other			
Other			
Other			
Other			
Other			

Know Your Operations

Your ability to respond quickly to any type of business disruption could make the difference between survival and closure.

Determine the maximum amount of time you can endure being closed after a disaster occurs by identifying your key business functions and processes, and decide how long you can go without being able to perform them.

Consider the following:

- What is your main product/service?
- How do you produce this product/service?
- What are the things that could most likely impact your ability to do business?
- If your business were impacted, who would you need to call? How would you reach them?
- What other business functions and processes do you perform to run your overall business?
- Which of these business functions and processes have legal, contractual, regulatory or financial obligations?
- Can the function be performed off-site? What equipment is needed?
- How much downtime can you tolerate for each function?
- What are the consequences if the function cannot be performed?
- Can your business survive without a specific function?

RECOMMENDATIONS:

Think about your employees and what activities they perform on a daily, weekly, monthly, and annual basis. Think about the functions and processes required to run your business in: accounting/finance; production/service delivery; sales/marketing; customer service; human resources; administration; information technology; and purchasing.

About the Form

Rate each function with a priority level of Extremely High, High, Medium or Low, and complete a separate form for each one. Consider any workarounds methods or possible backups for each function. Determine whether there are any temporary processes that can be implemented until a permanent solution is available. Document detailed procedures for workarounds, including any additional resources required. It is important to establish a maintenance program to keep your plan's contents current and relevant - review your business functions and processes every six months.

Know Your Operations

Use this form to identify what business functions are critical to your business' survival. Duplicate the form for each business function.

Updated:

Next Review Date:

BUSINESS FUNCTION:

Priority: ☐ Extremely High ☐ High ☐ Medium ☐ Low

Employee in charge:

Timeframe or deadline:

Money lost (or fines imposed) if not done:

Obligation: ☐ None ☐ Legal ☐ Contractual ☐ Regulatory ☐ Financial

Who performs this function? (List all that apply)

Employees:

Suppliers/vendors:

Key contacts:

(For additional space, use the Notes area below)

What is needed to perform this function? (List all that apply)

Equipment:

Special Reports/Supplies:

Dependencies:

(For additional space, use the Notes area below)

Who helps perform this function? (List all that apply)

Employees:

Suppliers/vendors:

Key contacts:

(For additional space, use the Notes area below)

Who uses the output from this function? (List all that apply)

Employees:

Suppliers/Vendors:

Key Contacts:

(For additional space, use the Notes area below)

Brief description of how to complete this function:

Workaround methods:

Notes:

Know Your Employees

Your employees are your business' most valuable asset. Suppose an emergency prevents access to your business.

- Would you know how to reach your employees?
- Do you have current home and mobile telephone numbers, addresses, email addresses, and emergency contact information?
- Is your employees' contact information available outside your business location?

Current employee contact information will enable you to reach employees to determine their safety and whereabouts, inform them about the status of your operations, where, when and if they should report, and what to do following a disaster.

Two-way communication with employees is critical before, during and after a disaster. Create an employee telephone calling tree and an emergency call-in voice recording telephone number, and know how to email and text your employees. Designate a telephone number where employees can leave messages.

Determine what assistance is needed for employees with disabilities or special needs, such as communications difficulties, physical limitations, equipment instructions and medication procedures. Determine whether employees are caring for individuals with special needs, which could prevent them from being available during a disaster. Identify employees who are certified in First Aid and CPR, and those with special skills that could be helpful during emergencies.

Employee preparedness can make the difference between whether your business is able to effectively recover from a disaster or not. Encourage employees to make personal emergency preparedness plans. The more prepared your employees are at home, the faster they will be able to return to work to help your business respond and recover from a disaster.

RECOMMENDATIONS:

To maintain your communication readiness, have your employees review and update their contact information at least every six months. Create a special emergency email account using free services provided by Yahoo, Gmail, Hotmail, etc., to enable people to contact the company regarding their status. Be sure all employees know how to access the emergency account.

About the Form

Document employee contact and emergency contact information and key responsibilities. Is there someone who can perform these functions during an emergency? Make sure that special skills are not known by only one person. It is important to establish a maintenance program to keep your plan's contents current and relevant - review your employee contact information every six months.

Know Your Employees

Use this form to record information about all employees, including the business owner so that each person can be contacted at any time. Duplicate the form for each employee.

Updated:

Next Review Date:

EMPLOYEE NAME:

Position/title:

Home address:

City, State, ZIP:

Office phone: Ext. Alternate phone:

Home phone: Mobile phone:

Office e-mail:

Home e-mail:

Special needs:

Certifications:

☐ First Aid ☐ Emergency Medical Technician (EMT) ☐ CPR ☐ Ham Radio

☐ Other:

☐ Special licenses:

Local Emergency Contact

Full name:

Relationship:

Home phone: Mobile Phone:

E-mail:

Out of State Emergency Contact

Full name:

Relationship:

Home phone: Mobile Phone:

E-mail:

Notes:

Know Your Key Customers, Contacts, Suppliers and Vendors

Preparedness planning is about being ready to manage any disruption to ensure the continuation of services to your customers. Your key customers need to know that you can provide "business as usual" even if others around you are experiencing difficulties. They will want to know that you are still in business or how soon you will be back and how the disruption will affect their operations. Maintaining up-to-date contact information for your key customers, contacts, suppliers, and vendors is critical.

The ability to resume your business operations relies on the capability of your suppliers and vendors to deliver what you need on time.

- Be sure your suppliers and vendors are not all in the same geographic location as you.
- Have alternate or backup suppliers and shippers in place.
- Request copies of your suppliers' business continuity plans.
- Establish a notification list and procedures.

Key contacts are those you rely on for administration of your business, such as:

- Accountant
- Bank
- Billing/Invoicing Service
- Building
  - Manager/Owner
  - Security
- Insurance Agent/Broker
- Insurance Company
- Internet Service Provider
- Payroll Provider
- Public Works Department
- Telephone Company
- Utilities

You may lose customers if you cannot meet their needs due to your own business disruption. After an event, it is important to keep customers informed about the status of your business, your product or service, delivery schedules, etc., and to develop mutually agreeable alternative arrangements.

RECOMMENDATIONS:

Identify various ways to communicate with customers after a disaster, such as direct telephone calls, a designated telephone number with a recording, text, e-mail, Twitter, Facebook, or announcements on your company website, by radio or through a newspaper.

About the Form

Be sure your customers know in advance how to obtain up-to-date information about the status of your business operations in the event of a disruption or major disaster.

Know Your Key Customers, Contacts, Suppliers and Vendors

Use this form to record information about your current suppliers, those you could use as an alternate choice and your key customers and contacts. Duplicate the form for each contact.

Updated:

Next Review Date:

CONTACT TYPE:

❑ Current Supplier/Vendor ❑ Back-Up Supplier/Vendor ❑ Key Customer/Contact

Company /Individual Name:

Account Number :

Materials/Service Provided:

Street Address:

City, State, Zip:

Company Phone:

Website:

Company Representative

Primary Contact:

Title:

Office Phone:

Mobile Phone:

E-mail:

Alternate Contact:

Title:

Office Phone:

Mobile Phone:

E-mail:

Notes:

Know Your Information Technology

Information and information technology (IT) are the lifeblood of most businesses, and must be included in your business continuity plan. Without access to your computer hardware, software, and digital data, your business operations can come to a standstill. It is likely that you communicate with or conduct business with your customers, partners, suppliers, and vendors via the Internet, which means your business is dependent on your computer system's connectivity and data communications.

Shut down and unplug all your computer hardware before an event to avoid serious damage due to power fluctuations. Consider elevating or moving equipment offsite. Have your employees take laptop computers home each day so they can work offsite if necessary.

Determine which data and records are vital to perform the critical functions identified in Know Your Operations section, and be sure they are backed up on one or more types of media. Store a backup copy onsite for use during small disasters, such as a failed hard drive, and store a second copy in a safe offsite location that can be easily accessed during large disasters.

Regularly backup your vital data and records. Move the backups to a different fire loss zone, safe deposit box or owner's home. The goal is to ensure your data and IT systems are available as you resume operations.

RECOMMENDATIONS:

Keep a backup copy of your computer's operating system, boot files, critical software, and operations manuals.

- Backup computer files, including payroll, tax, accounting and production records.
- Maintain an up-to-date copy of computer and Internet login codes and passwords.
- When possible, keep hard copies of critical virtual files offsite.
- Make arrangements with IT vendors to replace damaged hardware and software, and/or to set-up hardware and software at a recovery location.
- Request written estimates for rental or purchase of equipment, shipping costs and delivery times. Be sure to list these companies on your supplier and vendor form.
- When flooding is possible, elevate computer equipment stored on the floor.

About the Form

If your computer equipment is damaged or destroyed, you will need to lease or purchase new hardware and replace your software. Make a list of everything you would need to order. The important thing is to know what is needed to perform your critical business functions. It is important to establish a maintenance program to keep your plan's contents current and relevant - review your information technology information every six months.

Know Your Information Technology

Use this form to list the computer equipment, hardware and software, vital records and your back up processes that you will need to fulfill your critical business functions. Duplicate the form for each item or record.

Updated:

Next Review Date:

TYPE:

❑ Computer Equipment/Hardware ❑ Computer Software ❑ Vital Records

Item:

Title and Version/Model Number:

Serial/Customer Number:

Registered User Name:

Purchase/Lease Price: $

Purchase/Lease Date:

Quantity (equipment) or Number of Licenses (software):

License Numbers:

Technical Support Number:

Primary Supplier/Vendor:

Alternate Supplier/Vendor:

Notes:

Name of vital record:

Name of Business Function Vital Record Supports:

Type of Media:

Is It Backed Up?

How Often is it Backed Up?

Type of Media for Backup:

Where is it Stored?

Can the Record be Recreated?

Notes:

Know Your Finances

The time to prepare your business' finances is before a disaster occurs. Preparing your business financially now so it is ready to respond, recover, and continue operating when a business disruption occurs is just as critical as knowing exactly what to do when disaster strikes.

Here are some disaster preparedness ideas to consider:

Have an emergency cash reserve fund.

- You may need cash in order to purchase supplies or equipment, or relocate your business temporarily.

Have credit available.

- If you don't have enough cash in your emergency fund, be sure to have a line of credit or a credit card available.

Identify financial obligations and expenses that must be paid.

- You should not assume that because your area got hit by a disaster your suppliers, vendors and creditors are aware of the situation and are automatically granting extensions. Items such as mortgage, lease, or rental payments may still need to be made even after a disaster strikes your business.

Consider creating a policy regarding payroll during and after a disaster.

- Payroll is often overlooked in business continuity planning. You should not assume that your employees will continue to work without pay during or after a disaster. Be sure your employees are aware of your payroll continuity plans ahead of time in order for them to plan for their personal financial obligations.
- Establishing clear strategies and procedures for controlling costs, reporting information to appropriate groups and clearly budgeting for and tracking what is actually spent during a significant disruption can have a positive impact on the business' bottom line performance and recovery.

RECOMMENDATIONS:

It is critically important to protect your place of business, your contents and inventory, and/or your production processes with adequate insurance.

- Evaluate your insurance policies and meet regularly with your insurance agent/broker to be sure you understand your coverage, deductibles and limits, and how to file a claim.
- Most policies do not cover flood or earthquake damage and you may need to buy separate insurance for those events.
- Consider a policy that will reimburse you for business disruptions in addition to physical losses.
- Consider business income (or business interruption) and extra expense insurance. Even if you have to close your doors for a limited period, the impact on your revenue and net income can be substantial.
- Consider adding contingent business income coverage to your basic policy to be sure you are covered for expenses and loss of net business income, as well as income interruptions due to damage that occurs away from your premises, such as to your key customers, suppliers or utilities.

About the Form

Use the checklist when creating your financial strategy for your business resilience. It is important to establish a maintenance program to keep your plan's contents current and relevant - review your finances every six months.

Know Your Finances

Use this checklist to consider and plan for your business' financial needs in the event of a disruption.

Updated:

Next Review Date:

Overall Business Needs

Have you worked with your bank to set up a line of credit for your company?

Who is responsible to activate it and who has access to it?

How much cash would be needed to survive a 3-day, 5-day, 10-day, or longer shutdown?

For what purpose is the cash needed?

Will you have that cash on hand?

Who would make the decision to utilize the cash?

Who would have access to the cash?

Do you have sufficient cash to pay for various additional services that might be needed, such as janitorial or security services?

Do you have a company credit card that could be used for emergency purchases?

Who is authorized to use the credit card?

Will you be able to pay your bills/accounts payable?

Do you have procedures in place to accommodate a business disruption?

Will you be able to continue to accept payments from customers/accounts receivable?

Do you have procedures in place to accommodate a business disruption?

Have you identified an alternate location where you can work?

Human Resources

In the event of a widespread disaster, how will payroll be handled?

If your business is forced to shut down temporarily, will some or all employees continue to be paid?

For how long?

Will they be able to use their sick and/or vacation time without restriction?

Are there union considerations?

Have your employees been made aware of your policies that will be in place during a disruption?

If banks are closed, will your business provide payroll-cashing services?

What is your business' policy on cash advances, check cashing, and employee loans?

Will your employees be expected to work overtime?

Know When to Update Your Plan

For your plan to be successful when a business disruption occurs, it needs to be continually maintained and updated. One effective way to do this is to include business continuity planning anytime there are changes in your business or your location – basically, in every business decision you make. Keep your employees up-to-date with any plan changes as this will help when they need to put the plan into action, which in turn will reduce the negative impact to your business.

Maintenance is fairly straightforward. Repeat the following process every six months:

- Have your employees review the plan.
- Is anything out of date?
- Has all contact information been verified and updated?
- Have your procedures changed?
- Have there been any changes in business priorities?
- Have responsibilities changed?
- Document any changes.

Finally, test your plan and conduct exercises with your key employees. Until you test your plan for vulnerabilities you may not see where the gaps are in keeping your business going during a disruption. No plan or set of documents should remain sitting on a shelf.

Conducting exercises or drills are effective ways to test your plan, engage employees and train them. The following pages include an exercise that deals with a power outage. Once you learn the basics of conducting an exercise, you can easily generate your own scenario.

Another option to test your plan is to pose this scenario to employees at the end of a staff meeting: "If the alarm in this building were to go off, we would exit the building. Once outside we are told that we cannot go back into the building for one week. What would you do? How would you continue to work?" This will get people thinking about the possibilities and get them on board with your program. You may be surprised at your employees' increased level of growth and maturity when it comes to making the correct decisions following a disaster. This type of exercise can also be a great team building activity.

About the Form

Disaster exercises provide opportunities for you to: test company disaster readiness; train employees through practice; improve employees' ability to make informed decisions when responding to an emergency; identify what needs to be done during and after a disaster; and examine a specific scenario or situation more closely.

Gather your team, key employees and anyone else who would benefit from the exercise, present the power outage scenario, and begin the discussion with the questions provided. This can be done informally, such as during lunch or as part of a staff meeting.

Know When to Test Your Plan
Table Top Exercise: Power Outage Scenario

It is a hot, rainy Friday morning. The current time is 11:30 AM. Suddenly, the lights go out and all of the computers, printers, and copiers turn off. For a few seconds, there is silence before the chatter begins to pick up. One of your emergency lights comes on, but the rest are not working. While many of the offices have windows to provide minimal light, the majority of the hallways and interior rooms are left in the dark.

1. Take the first 10 minutes to discuss what you will do next.

It is now 1:00 PM and the lights still are not on. The building HVAC has been off now for 1 ½ hours and the temperature inside the building is gradually becoming unbearable. Your entire power grid is without power. There is no word from the electric company about restoration of power.

2. Now what are you going to do?
3. Is your technology/computer room being dealt with? By whom?
4. Has someone turned off all computers, printers, and equipment to prevent electrical surge when power is restored?
5. Is your phone system down? How are you going to manage the phone lines?

It is now 2:00 PM. Employees are asking if they can leave early. The word around town is that the power might not be restored for several days.

6. How will you communicate this message? What instructions will you convey to your employees? Customers? Vendors?
7. Are you going to declare a disaster in order to activate your business continuity plan?
8. Continue your discussion with the following questions:
9. How are people within the organization communicating with each other (e.g., sending and receiving messages, information, and response details)? How are they communication with other stakeholders (e.g., your customers and clients, the media)?
10. Is there a pre-determined and agreed upon central meeting place for company leaders, management, and employees?
11. Is there a copy of your business continuity plan that you can easily retrieve?
12. Are there any business processes for which there are manual workarounds? If so, discuss how that would happen.
13. How would you find an appropriate place to operate from for the remainder of the day? For the next one or two weeks, if necessary?
14. Have you begun an assessment that includes an evaluation of the status of employees, customers, operations, and external utilities?
15. How would you ensure that customer concerns are managed?
16. Have you begun to determine how much data was lost and how that will affect your operations?
17. Some employees are asking, "How will I know if I should come to work Monday?"

Know When to Test Your Plan
Table Top Exercise: Power Outage Scenario

It is now 7:30 AM on Monday, three days later. The power is still out and the Health Department has determined that "no building without running water can open for business." Clients are calling and the company voicemail system is full. Employees are texting the Human Resources Director asking for guidance.

18. What do you tell them?

Exercise Debrief:

19. What is missing from your plan?
20. What worked well in this scenario?
21. What did not work so well?
22. What could you do differently next time that would improve your response?
23. List the actions you will take to improve your plans.

Exercise Wrap Up:

This completes the exercise. In order to maximize what can be learned from this effort, have all participants write down their thoughts and concerns. You can address these and the debrief issues at future meetings.

Notes

Exercise Date:

Next Exercise Date:

Know Where To Go for Help

Your relationship with your community and outside agencies can strengthen your ability to protect your employees and property and return to normal operations. Maintain a channel of communication with community leaders, public safety organizations such as the police, fire and emergency medical services, government agencies, utility companies, and others. Working together with outside agencies can be beneficial because they can provide a wealth of information to help you recover quickly from a disaster.

Refer to the resources below for more information about implementing disaster safety recommendations to help you prepare for and recover from natural or other types of disasters.

Insurance Institute for Business & Home Safety

In addition to providing this free business continuity tool kit, IBHS provides free disaster preparedness and property protection guidelines, recommendations and projects for small businesses. The Institute also offers post-disaster recommendations on repairing and rebuilding to make your building(s) stronger and safer the next time a disaster strikes.

http://disastersafety.org

American Red Cross

Among other disaster preparedness and response services, the Red Cross offers a number of preparedness training programs and resources for workplaces, families, and individuals.

www.redcross.org

Business Civic Leadership Center – Disaster Help Desk

The BCLC Help Desk is designed to enhance community economic recovery after a disaster. The Help Desk provides on-the-ground coordination of information among businesses, local chambers of commerce, NGOs, government responders, and disaster recovery specialists.

https://www.uschamberfoundation.org/site-page/disaster-help-desk-business

DisasterAssistance.gov

Provides information on how you might be able to get help from the federal government before, during and after a disaster. If the President of the United States makes help available to individuals in your community after a disaster, you can visit this site to apply online.

http://www.disasterassistance.gov

Federal and Local Emergency Management Agencies

Even the largest, most widespread disasters require a local response. Local emergency management programs are the core of the nation's emergency management system.

https://www.fema.gov/emergency-management-agencies

Internal Revenue Service–Disaster Assistance and Emergency Relief for Businesses

The IRS offers audio presentations about planning for disaster. These presentations discuss business continuity planning, insurance coverage, record keeping and other recommendations for staying in business after a major disaster.

http://www.irs.gov/Businesses/Small-Businesses-&-Self-Employed/Disaster-Assistance-and-Emergency-Relief-for-Individuals-and-Businesses-1

Small Business Administration

The U.S. Small Business Administration provides loans, loan guarantees, contracts, counseling sessions and other forms of assistance to small businesses following a disaster.

http://www.sba.gov/

https://www.sba.gov/business-guide/manage/prepare-emergencies-disaster-assistance

Small Business Development Centers

The SBDC assists small businesses with financial, marketing, production, organization, engineering and technical problems, as well as feasibility studies.

http://www.sba.gov/content/small-business-development-centers-sbdcs
http://www.asbdc-us.org/

Acknowledgments

The staff of IBHS wishes to acknowledge the valuable input of all those who assisted in producing this toolkit. In particular, we extend thanks to:

- Steve Elliot, President & CEO, Elliot Consulting
- Frantz Joachim, CBCP, Director of Risk Management, AmeriLife
- Tim Lovell, Executive Director, Tulsa Partners, Inc.
- Mark R Lupo, CBCP, Area Director, The University of Georgia SBDC of Columbia
- David Maack, CEM, CPM, WCEM, Coordinator, Racine County Office of Emergency Management
- Lisa Marino, CBCP, Enterprise Business Continuity Management, Mercury General Corporation
- Howard Pierpont, Chairman of the Board, The Disaster Preparedness and Emergency Response Association [DERA]
- Marcus Pollock, Chief, Standards and Technology, National Integration Center, FEMA, DHS
- James Price Jr., MBCP, MBCI, ITIL, CEO, 3J Contingency Planning Services
- Bob Roberts, Emergency Manager, Tulsa Public Schools
- Sonia Singh, Emergency Preparedness Coordinator, City of Markham, Canada
- Judith Warren, Regional Coordinator, Humboldt State University, Office of Distance and Extended Education

Feedback

IBHS welcomes your feedback and comments about the OFB-EZ recovery planning toolkit, including the usefulness of your plan when a business disruption or workplace disaster occurs. Your feedback will help IBHS improve the tool for future users, and your story may help encourage others to develop a business continuity plan. Please send any feedback to info@ibhs.org.

OFB-EZ is a program of the Insurance Institute for Business & Home Safety
Download this document at DisasterSafety.org/open-for-business

A PROGRAM OF IBHS

SEVERE WEATHER: EMERGENCY PREPAREDNESS AND RESPONSE PLANNING

Prepared by the Insurance Institute for Business & Home Safety (IBHS), an independent, nonprofit, scientific research and communications organization supported by the property insurance industry. IBHS works to reduce the social and economic effects of natural disasters and other risks on residential and commercial property by conducting building science research and advocating improved construction, maintenance and preparedness practices.

Insurance Institute for Business & Home Safety®

Contents

Overview

Many businesses are not prepared to respond to man-made or natural disasters. Statistics show that of the businesses that close because of a disaster, at least 1 in 4 never reopens. Small businesses are particularly at risk because they likely have all of their operations concentrated in one location that could be damaged or destroyed.

To help keep small businesses "open for business," IBHS developed this severe weather emergency preparedness and response planning toolkit. It is designed as a stand-alone guide, along with a customizable checklist, that can be used by any small business to build a plan for responding to operational disruptions. It also complements IBHS' OFB-EZ® program, which is a simple-to-use business continuity program that focuses on recovering after the initial emergency response (DisasterSafety.org/ibhs-business-protection/ofb-ez-business-continuity). To be best prepared, businesses should implement both programs to protect their businesses and bottom lines.

What Is an Emergency Preparedness and Response Plan?

A way of organizing and implementing actions to prevent or reduce damage from natural disasters and other extreme events.

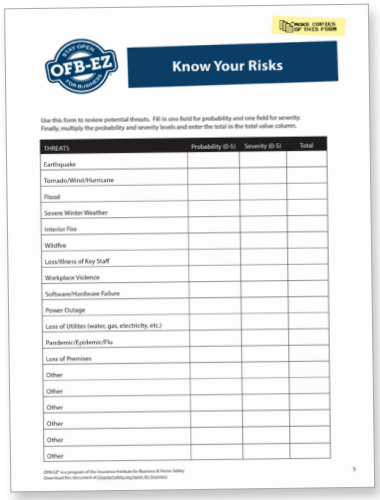
WHY CREATE AN EMERGENCY PREPAREDNESS AND RESPONSE PLAN?

Every business that wants to stay in business should have a plan to prepare for and respond to severe weather and other emergencies. Not having a plan, or having a poorly prepared or misunderstood plan, can lead to disorganized preparation or confused response, with the possibility of harm to employees, facilities, equipment or operations. The highest priority should be employee safety, but it also is important to reduce property damage and economic loss. Having a plan saves time and focuses energy when facing an imminent crisis, or when responding to one that could not have been foreseen in advance. In addition to planning for severe weather that threatens an entire region, preparedness and response plans can also be created for non-weather-related threats and other hazards that are specific to one business, such as water damage from a leaking or bursting pipe, a small fire or a power outage.

WHAT SHOULD BE INCLUDED IN AN EMERGENCY PREPAREDNESS AND RESPONSE PLAN?

All plans should include "best practices" to be taken before, during and after an emergency, along with actions to address unique challenges that are specific to each business' facilities and operations, and the risks it faces.

In addition to severe weather plans, it is also important to consider non-weather-related threats and risks that stem from the nature of the business, such as hot work operations, metalworking and woodworking, manufacturing, flammable liquids handling and storage, plastics storage, cooking equipment, refrigeration systems, and other


OFB-EZ

Know Your Risks

Use this form to review potential threats. Fill in one field for probability and one field for severity. Finally, multiply the probability and severity levels and enter the total in the total value column.

THREATS	Probability (0-5)	Severity (0-5)	Total
Earthquake			
Tornado/Wind/Hurricane			
Flood			
Severe Winter Weather			
Interior Fire			
Wildfire			
Loss/Illness of Key Staff			
Workplace Violence			
Software/Hardware Failure			
Power Outage			
Loss of Utilities (water, gas, electricity, etc.)			
Pandemic/Epidemic/Flu			
Loss of Premises			
Other			
Other			
Other			
Other			
Other			
Other			

business-related risks of greatest concern to each business. The "Know Your Risks" exercise in the OFB-EZ toolkit will assist in determining the threats that are likely to affect your business, taking into account the frequency (the likelihood the event will occur) and the severity (the amount of damage the event is capable of causing the business). Businesses should plan for the highest ranking threats as soon as possible.

The next step is to inspect the vulnerable areas of your building envelope (roof, windows, walls and doors), surrounding premises, worksite layout and emergency systems, to ensure your plan protects the most vulnerable assets and operations. This analysis also may help to identify ways to streamline the planning process from a time and money perspective.

Once these basic organizational tasks have been completed, the next step is to identify and implement the steps needed to protect people and property. Most storms and many other types of natural hazards can be tracked and monitored, which allows for at least some preparedness planning. However, when that is not the case, emergency planning will help make businesses more resilient and better able to withstand even an event that happens without warning.

GET PREPARED

CREATE YOUR SEVERE WEATHER AND OTHER TYPES OF EMERGENCY PREPAREDNESS & RESPONSE PLANS

Based on this guide's recommendations, your type of business and other available resources, use the customizable checklist template (which can be downloaded at DisasterSafety.org/wp-content/uploads/2016/04/ez-prep-checklist-template-ibhs.xls) to create your plan, including preparedness and recovery actions and tasks, team members' responsibilities, alert levels, etc., to fit your business and building needs.

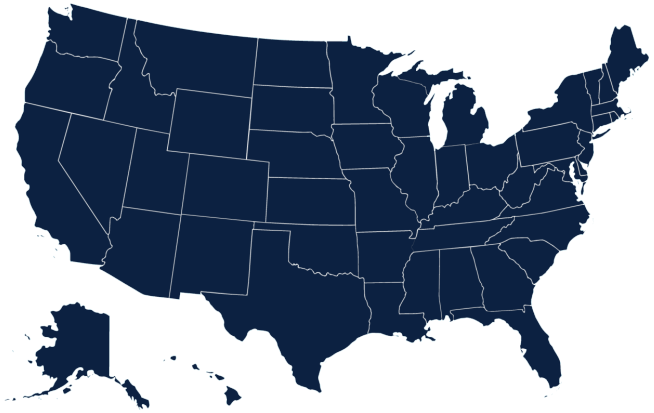
UNITED STATES NATURAL DISASTER AND SEVERE WEATHER SEASONS

Ideally, emergency planning is a 12-month priority. However, at minimum, the weeks before the start of a severe weather season in your area are a good time to refocus your efforts.

Natural Disaster	Seasons	Geographic Location
Severe Winter Weather	Nov. 1–Mar. 1	Northeast, Midwest, Mountain West, Northwest, High elevation in Southeast and Mid-Atlantic
Flooding	Mar. 1–June 30	Northwest, Mountain West, Northwest, Midwest
Flash Flooding	Year-round	Nationwide
Tornadoes	Mar. 1–June 30	Midwest, Southeast, Southwest, Mid-Atlantic
Hurricanes	June 1–Nov. 30	Gulf Coast and Atlantic Seaboard States
Thunderstorms and Lightning	Mar. 1–Sept. 30	Central Plains, Southeast, Mid-Atlantic, Southwest
Hailstorms	Mar. 1–September 30	East of the Rockies
Wildfire	Mar. 1–June 1	Southeast
	June 1–Nov. 1	Mountain West, Pacific West, Southwest

DISCOVER YOUR RISKS

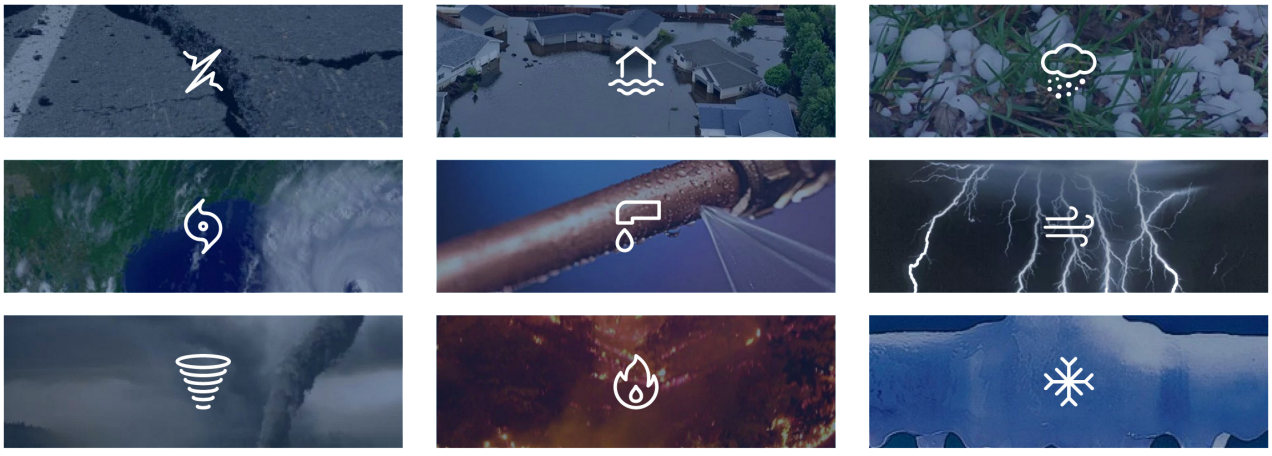
To help identify natural hazards that may affect your business, use IBHS' ZIP Code tool at DisasterSafety.org. Enter your ZIP Code and select "Go" to see severe weather risks of your location. Then select a specific risk to get the free disaster preparedness resource including practical, specific measures business business owners can take to help minimize the impact of disaster.



Discover the risks you face.

Click your state on the map
or enter your Zip Code below.

zip code GO



LIFE SAFETY

LIFE SAFETY COMES FIRST

Business owners and managers should promote and encourage disaster safety and personal preparedness among employees—for example, posting "how to" materials in the workplace, encouraging employees to create a family disaster plan, and conducting educational or training programs. These efforts can be conducted online, face-to-face, or through brochures/handouts, videos, etc.

Emergency preparedness and response plans should include the following safety procedures. Each task should be assigned to either a title/position or an individual along with an alternate. These assignments should be reviewed and updated annually.

COMPLETED	Life Safety Tasks	Primary Staff Responsible	Alternate Staff Responsible
☐	Create procedures on how employees are to report emergencies (fire alarm, dialing 911, calling an internal emergency number, etc.).		
☐	Create medical emergency procedures (who can perform them and to what extent, or whether your business will rely on the fire department or ambulatory services to provide these services).		
☐	Create evacuation procedures (appoint a lead or team to be in charge of developing evacuation plans including how to evacuate and what routes to take, including floor plans with exit diagrams, and actions employees should take before and while evacuating such as shutting windows, turning off equipment, and closing doors behind them; the plan should also include procedures on how to account for all employees after an evacuation—e.g., sweep the area, check offices and restrooms, conduct roll call in the assembly area, etc.).		
☐	Create shelter-in-place procedures (what actions employees should take before and while sheltering).		
☐	Create life safety equipment maintenance procedures (AED, personal protection equipment, etc.).		
☐	[Insert additional rows for your own specific action items or tasks]		

OFF-SEASON

Every region of the county is at risk for severe weather during at least some seasons of the year. Ideally, emergency planning is considered a 12-month priority, but even if that is not the case, the weeks before the start of a severe weather season in your area is a good time to refocus your efforts.

COMPLETED	Off-Season: [Month - Month] Tasks	Primary Staff Responsible	Alternate Staff Responsible
☐	Create emergency response teams, including a chain of command, a current list of telephone numbers and contacts for emergency plan team members, local police and fire departments, utilities, contractors, HVAC contractor, electrician, plumber, building owner, if applicable, etc.		
☐	Create checklists for all employees, specifically for those who have assigned responsibilities. Be sure to assign primary and alternates for each action/task.		
☐	Designate a knowledgeable person who will be responsible for monitoring the news and weather, and for disseminating weather updates.		
☐	Assemble needed supplies for an emergency supply kit and first aid kit. If employees are to remain on site in safe conditions, ensure proper supplies such as food, bedding and life safety equipment are included. Be sure to reinspect and replenish supplies annually or after an actual emergency.		
☐	Create emergency shutdown and start-up procedures with appropriate personnel for components such as computer systems, special equipment, refrigeration systems, etc., and for building systems such as electric systems, gas and/or other utility systems, HVAC and boilers. Review procedures annually.		
☐	Establish a relationship in advance (thereafter, revisit relationship) with local, reliable contractors that will be available for post-storm building repairs.		
☐	Inspect the building envelope (roof cover, flashing, windows, walls, warehouse doors) and conduct repairs.		
☐	If located in a flood or storm surge zone, determine water entry points and document flood protection techniques.		
☐	Inspect and conduct repairs of surrounding grounds to ensure proper site drainage, including ground drains and gutters to facilitate water runoff.		

OFF-SEASON (CONT.)

COMPLETED	Off-Season: [Month - Month] Tasks	Primary Staff Responsible	Alternate Staff Responsible
☐	If backup power such as a diesel generator is to be used, test the system and establish proper contracts with fuel suppliers for emergency fuel deliveries.		
☐	Maintain fire sprinkler systems, fire extinguishers and smoke detectors. Consider a fire protection system that is monitored so the fire department is immediately notified when the sprinklers are activated.		
☐	Inspect and replenish critical spare parts inventory.		
☐	Consider replacement contingencies (i.e., equipment leasing contracts or plans) for critical business equipment that can cause a bottleneck in business operations or may take extensive time to replace.		
☐	For production facilities, back up capabilities by adding additional production lines, shifts, outsourcing, etc.		
☐	Create a system to communicate after an emergency such as message templates for the business' website, telephone recording, social media sites, company intranet, employee communications, etc. Maintain a list of local radio and TV stations in the event the business needs to broadcast information on closings/reopenings.		
☐	Create and disseminate a payroll policy in the event of office closings due to an emergency.		
☐	Consider how documents, records and reports (both hard copies and electronic copies) will be safeguarded including storing in fire-rated cabinets, relocating records above ground level, bolting cabinets in earthquake areas, transferring to an off-site location, backing up at a distant location, etc.		
☐	[Insert additional rows for your own specific action items or tasks]		

5 DAYS BEFORE AN INCIDENT

COMPLETED	5 Days Before [Incident] Tasks	Primary Staff Responsible	Alternate Staff Responsible
☐	As needed, secure equipment, cabinets and fixtures vulnerable to the approaching event.		
☐	Inspect the roof and grounds for loose debris which may become a hazard in high winds. If staff or temporary help is available, begin removal of the debris; otherwise, the removal may be done at the 72-hour interval.		
☐	Notify employees of the potential for severe weather, and instruct them to prepare for the possible implementation of the emergency plan.		
☐	Ensure all employees have the business' designated emergency telephone numbers, key contact information and other important documents such as an employee emergency wallet card, telephone call tree list, etc.		
☐	[Insert additional rows for your own specific action items or tasks]		

72 HOURS BEFORE AN INCIDENT

COMPLETED	72 Hours Before [Incident] Tasks	Primary Staff Responsible	Alternate Staff Responsible
☐	Check that all roof equipment (air conditioners, fan housing, satellite dishes, antennas and signs) mounts are secure against damage during heavy winds.		
☐	Inspect and repair roof edge flashing. Clear roof drains, gutters and downspouts of debris to prevent water backup.		
☐	Remove or secure all loose ground items, including landscaping that may become windborne debris. Secure garbage cans, outdoor furniture, signs, awnings, flags and flagpoles, and tools.		
☐	Clean out all debris from outdoor perimeter drains, especially in areas where water may collect such as shipping and receiving areas where the ground slopes toward the building.		
☐	Ensure fire protection systems are in proper working order.		
☐	Fill emergency generators with fuel and contact fuel suppliers with anticipated needs for post-storm deliveries.		
☐	Review message templates for business' website, telephone recording, employee communications, intranet, etc.		
☐	Advise employees to begin checking the employee emergency hotline, business' website, company intranet, etc., for updates on the status of the office/ facility.		
☐	Instruct employees with laptops to take them home at the end of each day and confirm they can connect to the business' server from home. In addition, instruct all employees to fully charge their cell phones and any other common devices, and to ensure they have a power cord and car charger.		
☐	[Insert additional rows for your own specific action items or tasks]		

24–48 HOURS BEFORE AN INCIDENT

COMPLETED	24–48 Hours Before the [Incident] Tasks	Primary Staff Responsible	Alternate Staff Responsible
☐	Make decision on when to close office/facility and to excuse employees so they have sufficient time to prepare their homes and families, and notify employees of office closure details.		
☐	Notify key customers, suppliers and partners of the office/facility closing (i.e., USPS, Fed Ex, UPS, cleaning service, building management, vendors, shippers, etc.).		
☐	For hurricanes and other high-wind events, install window protection (e.g., permanent shutters or plywood panels; tape should never be used to protect against pressures and flying debris). If window protection is unavailable, close all window blinds, and cover office equipment with plastic sheets or tarps.		
☐	Disconnect all electrical equipment and unplug from power source.		
☐	If building has the potential of being exposed to flooding or storm surge, seal all water entry points (i.e., utility penetrations into the building) and install flood protection including first-floor drain plugs.		
☐	Raise equipment and furniture above expected flood level heights, and elevate or relocate critical records, computers and equipment to an alternate site, if possible.		
☐	If employees are to remain on site, make sure a safe and secure area is designated in advance. If conditions permit, instruct them on how to monitor, document, and minimize leaks and water infiltration in critical areas with vital equipment.		
☐	If expecting any deliveries, contact sender/shipper to inform them of office/facility closure.		
☐	Make sure employees with "call tree" responsibilities have the most updated version of the company telephone call list and that they have it in multiple formats (hard copy, electronically, etc.).		
☐	Instruct employees to change their voicemail and turn on their email "out of office" notification to indicate the office/facility is closed due to weather, etc.		
☐	Customize the message template's message and post to business' website, social media sites and company intranet, and record outgoing message for the business' main telephone line, the employee emergency hotline, etc.		

24–48 HOURS BEFORE AN INCIDENT (CONT.)

COMPLETED	24–48 Hours Before the [Incident] Tasks	Primary Staff Responsible	Alternate Staff Responsible
☐	Advise employees to check on the status of the office/facility at least twice per day.		
☐	Place a "closed" notice on office/facility main entrance (including instructions on how to find out more information online or by phone).		
☐	Conduct full or partial shutdown procedures.		
☐	Close and lock all office doors, especially perimeter offices.		
☐	[Insert additional rows for your own specific action items or tasks]		

DURING AND IMMEDIATELY AFTER AN INCIDENT

COMPLETED	During & Immediately After [Incident] Tasks	Primary Staff Responsible	Alternate Staff Responsible
☐	While building cannot be occupied, if alarm system loses power, arrange alternate security.		
☐	Activate the company telephone call tree process to contact all employees regarding the status of the business' office/facility.		
☐	Update employee emergency hotline, company intranet, social media and business website with postings on the status of the business' operations.		
☐	Designate times for key staff members to call into conference calls for situation overviews.		
☐	[Insert additional rows for your own specific action items or tasks]		

RECOVERY AFTER AN INCIDENT

COMPLETED	Recovery After [Incident] Tasks	Primary Staff Responsible	Alternate Staff Responsible
☐	Authorize employees with assigned recovery responsibilities to return to the facility, assess conditions, document damages, and notify the business owner, key managers, etc., of their findings.		
☐	When it is deemed safe, authorize employees with assigned start-up responsibilities to begin the documented start-up procedures.		
☐	Take an overall inventory, including photos of all damaged property, and report damage and related expenses to your insurance company.		
☐	Where possible or necessary, protect building, equipment and furniture from further damage.		
☐	Instruct employees returning to the building to examine their work area, test all office equipment and report findings back to the designated staff contact. Notify key customers, suppliers and partners of office/facility reopening and any necessary property or operational changes resulting from storm damage.		
☐	When all safety and operational concerns are addressed, provide an "all clear" so employees can return to work.		
☐	[Insert additional rows for your own specific action items or tasks]		

LONGER-TERM PLANNING AND REPAIRS

Once a business gets through a major disruption, it is important to remember the next catastrophe can occur at any time. Now is the time to begin inspecting the building and premises, initiating repairs to the building envelope, and making improvements that will help to reduce damage in the future. IBHS provides a wealth of resources on strengthening buildings against natural hazards at DisasterSafety.org/fortified/safer-business and DisasterSafety.org/ibhs-business-protection.

This is also the time to hold a debrief meeting to review procedures, solicit input from employees on what was successful and what was not, and document any shortcomings of the emergency plan. Compile a log of actions to be taken and incorporate improvements into the plan for the future. The employees' ability to safeguard themselves and the business in an emergency reflects their understanding of the overall plan and their own responsibilities, so practice during the off-season so everyone is prepared when the next storm hits and the plan must be implemented.

COMPLETED	Long-Term Planning & Repairs Tasks	Primary Staff Responsible	Alternate Staff Responsible
☐	Hold a debrief meeting noting successes and failures, compile a log of actions to be taken, and incorporate improvements into plan.		
☐	[Insert additional rows for your own specific action items or tasks]		

THE IMPORTANCE OF TRAINING & EXERCISING

Once the plan and checklists are completed, review, train and rehearse with employees so they can fulfill their roles and responsibilities. The emergency preparedness and response plan should not be kept a secret. It should be shared with the entire staff and feedback should be encouraged throughout the entire process. Employees who are included in the process and made aware of the plan will have the desire and be more equipped to assist with recovery in the event of an approaching storm or other type of business interruption. Every employee should know what their role is and what is expected of them.

- Exercise the plan annually and incorporate feedback, gaps and lessons learned in the annual update.
- Distribute the plan and checklists in both paper and electronic formats to all employees.

BUSINESS & OFFICE EMERGENCY DISASTER KIT

Part of developing an emergency preparedness and response plan is the assembly and maintenance of a business/office emergency disaster kit and supplies. Some disasters may require employees to shelter-in-place; other times, emergency personnel may need to stay on site in order to protect the property and building. Having the essential items such as water, food, communication tools, hygiene, sanitation and first aid supplies could be critical to avoiding injury to employees and reducing damage to your business.

Use the suggested items on the supply list to help assemble the emergency preparedness and response supplies that may be needed.

SUPPLY CHECKLIST

EZ-PREP SUPPLY CHECKLIST

Download at DisasterSafety.org/wp-content/uploads/2016/04/ez-prep-supply-checklist-ibhs.xls.

COMPLETED	Long-Term Planning & Repairs Tasks	Type	Quantity Needed	Quantity Present	Date Checked
EQUIPMENT					
☐	Batteries				
☐	Battery-powered items (TV, lanterns, personal fans, etc.)				
☐	Boots				
☐	Bungee cords				
☐	Camera (digital, disposal, and/or smartphone with camera)				
☐	Communication devices (two-way radios, satellite radios, cell phones, chargers and weather radio)				
☐	Electrical lockout/tagout kits				
☐	Extension cords (indoor and outdoor)				
☐	Fire extinguishers				
☐	Floor drain plugs				
☐	Fuel cans and generator fuel				
☐	Hard hats				
☐	Hoses				
☐	Ropes				
☐	Safety harness				
☐	Shop vacuums (wet/dry)				
☐	Steel cables and turn buckles				
☐	Straps				
☐	Tape (duct, masking, electrical, cloth, caution, etc.)				
☐	Tarpaulins (water-resistant, fire-retardant, etc.)				
☐	Tools (pliers, hammer, gas wrench, wrenches, screwdrivers, nails, handsaw, staple gun, staples, etc.)				
☐	Utility knives				
☐	Yard equipment (axes, blowers, hatchets, pruners, trimmers, chainsaws, etc.)				

SUPPLY CHECKLIST (CONT.)

COMPLETED	Long-Term Planning & Repairs Tasks	Type	Quantity Needed	Quantity Present	Date Checked
CLEANUP					
☐	Bleach				
☐	Brooms and mops				
☐	Buckets/pails				
☐	Disinfectants				
☐	Eye protection (safety goggles)				
☐	Gloves (leather, nitrile, rubber, latex, etc.)				
☐	Ladders				
☐	Rakes and shovels				
☐	Spill kits				
☐	Towels (paper, cloth rags, etc.)				
☐	Waste drums				
SHELTER-IN-PLACE					
☐	Battery-powered or hand-crank radio and a NOAA Weather Radio with tone alert and extra batteries for both*				
☐	Bedding and blankets				
☐	Can opener (manual)				
☐	Coolers and ice				
☐	Disposable plates, cups and eating utensils				
☐	Drinking water in non-breakable containers				
☐	Dust mask to help filter contaminated air and plastic sheeting and duct tape to shelter-in-place*				
☐	First-aid kit*				
☐	Flashlight*				
☐	Food (at least a three-day supply of non-perishable food)*				
☐	Hand sanitizer				
☐	Local maps*				
☐	Plastic bags (zip-top, trash, etc.)				
☐	Toiletries				
☐	Manual can opener for food*				

SUPPLY CHECKLIST (CONT.)

COMPLETED	Long-Term Planning & Repairs Tasks	Type	Quantity Needed	Quantity Present	Date Checked
☐	Moist towelettes, garbage bags and plastic ties for personal sanitation*				
☐	Water (one gallon of water per person per day for at least three days) for drinking and sanitation*				
☐	Whistle to signal for help*				
STORM/FLOOD PROTECTION					
☐	Sand and sand bags				
☐	Sealants (expandable polyurethane, caulk, caulk guns, etc.)				
☐	Sump pumps				
☐	Wood (plywood, lumber, etc.)				
☐	[Insert additional rows for your specific needed supplies]				

*Supplies suggested by Ready.gov

Notes

Notes

U.S. Secret Service creates cyberfraud task force

Cybersecurity
Monday, July 13, 2020

In recognition of the growing convergence of cyber and traditional financial crimes, the U.S. Secret Service is formally merging its Electronic Crimes Task Forces (ECTFs) and Financial Crimes Task Forces (FCTFs) into a single unified network, which will be known as the Cyber Fraud Task Forces (CFTFs). The mission of the CFTF is to prevent, detect, and mitigate complex cyber-enabled financial crimes, with the ultimate goal of arresting and convicting the most harmful perpetrators.

Since March, the Secret Service has focused its investigative efforts on disrupting and deterring criminal activity that could hinder an effective response to the pandemic and to recover stolen funds from Americans. The CFTF model has allowed for better data sharing, institutional alliance, and investigative skill development, the agency said in a statement announcing the moves.

Through these efforts, the Secret Service successfully has disrupted hundreds of online COVID-19 related scams, investigated a number of cyberfraud cases, halted the illicit sales of online stolen COVID-19 test kits, prevented tens of millions of dollars in fraud from occurring, and is leading a nation-wide effort to investigate and counter a vast transnational unemployment fraud scheme targeting the U.S. state unemployment programs.

In the past, cybercrime investigators required added training to conduct computer forensic investigations, exams, trace IP addresses, and work in conjunction with private technological companies. Meanwhile, traditional financial crimes investigators worked to secure and protect the financial infrastructure by tracking fraudulent wire transfers, counterfeit checks, and combating counterfeit currency.

In today's environment, no longer can investigators effectively pursue a financial or cybercrime investigation without understanding both the financial and internet sectors, as well as the technologies and institutions that power each industry, the agency stated. Secret Service investigations today require the skills, technologies, and strategic partnerships in both the cyber and financial realms. Nearly all Secret Service investigations make use of digital evidence, and the greater technological sophistication by bad actors has led to a proliferation of blended cyber-enabled financial crimes.

Through the creation of the CFTFs, the Secret Service said it aims to improve the coordination, sharing of expertise and resources, and dissemination of best practices for all its core investigations of financially motivated cybercrime. The CFTFs will leverage the combined resources and expertise of both the ECTFs and FCTFs to collaboratively investigative the range of cyber-enabled financial crimes, from

business email compromise scams to ransomware attacks, from data breaches to the sale of stolen credit cards and personal information on the Internet.

The Secret Service has 42 domestic CFTF locations with two international locations, London and Rome. In the coming years, the Secret Service plans to further extend the CFTF network to encompass 160 offices across the country and around the globe.

Today's other top stories

Insured sues title agency over condominium issues

Georgia will continue RIN into August

FinCEN issues advisory on COVID-19 related schemes

Kansas notarization order extended to September

Arizona gets new insurance department director

COMMENT BOX DISCLAIMER:

October Research is not responsible for the comments posted on its websites by readers. We will do our best to remove comments that include profanity or personal attacks or other inappropriate comments.

Comments:

Be the first to leave a comment.

Leave your comment

NALA | THE PARALEGAL ASSOCIATION

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. 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
2.0	Protecting NPI - Pillar 3 / Linda Monaco	*Linda Monaco*

Name of CP (Please Print)				NALA Account Number (On Mailing Label)
				149113
Signature of CP				Name of Seminar/Program Sponsor
				Protecting NPI - Pillar 3 / Attorneys' Title Fund Services, Inc.
Address				Authorized Signature of Sponsor Representative
				Linda Monaco
				Date of Educational Event:
City:		State (XX):		
Preferred e-mail address				Location:
				Recorded Webinar

For Office Use Only	
Substantive hours	
Non-substantive hours	
Ethics	

FL BAR Reference Number: 2504054N

Title: Protecting NPI – Pillar 3

Level: Intermediate

Approval Period: 06/01/2025 - 12/31/2026

CLE Credits

General	2.0
Ethics	1.0
Technology	1.0

Certification Credits

Real Estate	2.0