RECENT DEVELOPMENTS IN PROFESSIONAL LIABILITY AND REGULATORY COMPLIANCE

- **Robert N. Young, Director**
- **Trisha L. Barfield, Associate Attorney**
- **Carruthers & Roth, P.A.**
- **Email: rny@crlaw.com , tlb@crlaw.com**
- **Phone: (336) 478-1131, (336) 478-1176**

1

TOPICS

1. Amendments to the North Carolina Identity Theft Protection Act and other cybersecurity issues;
2. Responding to a subpoena;
3. Recent decisions regarding accountant professional liability; and
4. Recent enforcement of workers compensation laws by the North Carolina Industrial Commission.

2

CYBERSECURITY

3

CYBERSECURITY TOPICS

1. Threats to business's data;
2. Legal obligations regarding data and amendments to the NCITPA;
3. Other state data protection and breach laws; and
4. Ways to protect your business.

4

COMMON THREATS TO BUSINESS'S DATA

Cyber Threats

Email

Internet/websites

Ransomware (i.e. NC State BAR)

Stolen or lost devices containing data

5

LARGEST CYBER THREAT: (P.I.C.N.I.C.)

PEOPLE

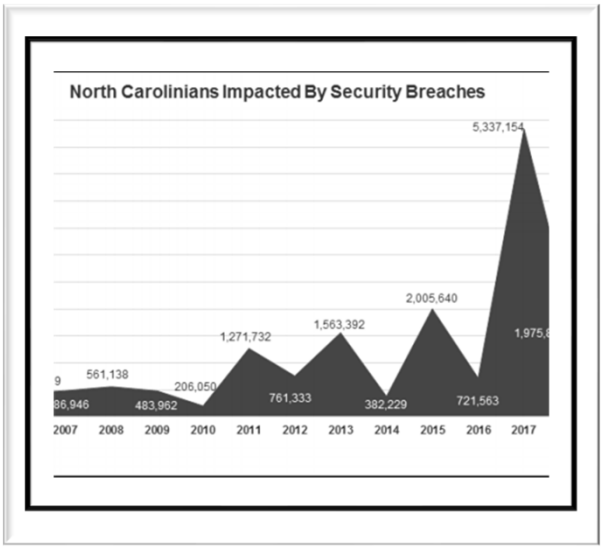
6

NC DOJ 2018 DATA BREACH REPORT

- In 2018, organizations reported 1,057 data breach notices affecting more than 1.9 million NC residents.
  - Increase of 3.4% from 2017.
- Phishing scams up 11% and constitute 26% of all breaches.
- Almost 40% of all breaches included email.

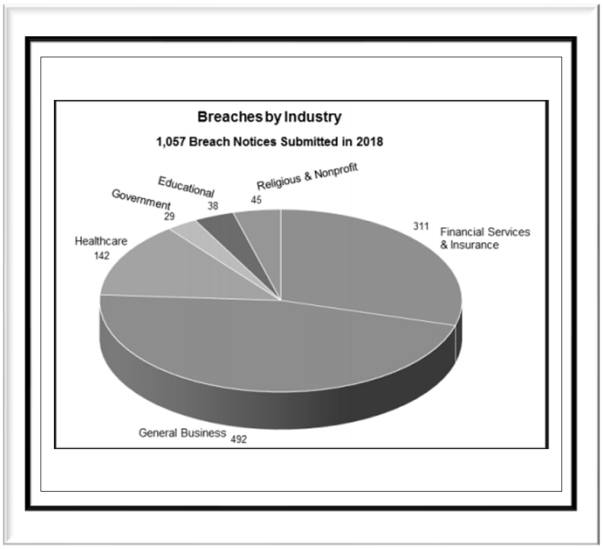
7

NC DOJ 2018 DATA BREACH REPORT



8

NC DOJ 2018 DATA BREACH REPORT



9

LEGAL OBLIGATIONS REGARDING CLIENT INFORMATION DEPEND ON THE NATURE OF THE BUSINESS, WHERE YOU DO BUSINESS, AND WHERE YOUR CLIENTS RESIDE.

1. HIPAA: (medical practices and business associates that handle protected health information or PHI.)

2. Gramm- Leach-Bliley Act (GLBA): (financial institutions)

a. Enforced by the FTC

b. Applies to CPA's and tax preparers

c. **Safeguards Rule:** generally requires measures in place to keep customer information secure including developing a written security plan appropriate for size, complexity of business that includes:

1. A designated head of security program

2. Identify and access risks to customer information.

3. Design and implement a safeguard program and test it.

4. Use service providers that maintain safeguards.

5. Evaluate and adjust program as needed.

d. **Privacy Rule:** provide notice of privacy policy and practices to customers regarding nonpublic personal information.

e. **ALL GLBA obligations for financial institutions are <u>in addition to</u> obligations under NC and other data protection and breach notification laws.**

3. Contractual obligations.

4. North Carolina Identity Theft Protection Act (NCITPA)

5. Other state's data breach statutes in states where your clients reside, or you do business.

10

NORTH CAROLINA IDENTITY THEFT PROTECTION ACT: ("NCITPA")

- Effective December 1, 2005
- Generally obligates **all businesses that do business in NC or maintain personal information of NC residents** to safeguard client's personal information.
- Properly dispose of records with personal information.
- Notify affected individuals in the event of a breach.
- Provides private right of action if individual suffers actual damages.

11

AMENDMENT TO NCITPA

PROPOSED AMENDEMENT:

- House Bill 904, most recent version submitted 4/16/19: If passed, NCITPA to include more protected confidential information (i.e. medical information) and stricter requirements regarding breach determination and notification.
  - Like many other states and consistent with the national trend, creates **affirmative duties** to protect customer information in addition to data breach notification.

12

HB 904 AMENDMENT TO NCITPA: POLICY REQUIREMENT

- Major proposed changes:
- 1. Expressly requires **all businesses** to **implement and maintain reasonable security procedures and practices** appropriate to the nature of the personal information in the size, complexity and capabilities of the business, to protect personal information from unauthorized access, destruction, use, modification or disclosure.
  - Includes having appropriate written policies in place regarding the protection of personal information and data breaches.

13

HB 904 AMENDMENT TO NCITPA: BREACH NOTIFICATION

- 2. Breach notification timing updated from "without unreasonable delay" from discovery of breach to 30 days after discovery of the breach "*or reason to believe a breach has occurred*."
- 3. Must provide NC Consumer Protection Division notice of the breach, including:
  - (1) A description of policies in place regarding breaches;
  - (2) Steps taken to rectify the breach;
  - (3) A copy of the police report;
  - (4) Summary of the incident report;
  - (5) Summary of computer forensic report if done; and
  - (6) Information regarding notice to affected individuals.

Amended version clarifies that if entity in compliance with HIPAA regarding notification, then in compliance with amended NCITPA, but NOT GLBA.

14

HB 904 AMENDMENT TO NCITPA: CREDIT MONITORING

- 4. A business who knows that a customer's social security number has been disclosed must contract with a third-party to offer the consumer credit monitoring services for a period of not less than two years.

15

HB 904 AMENDMENT TO NCITPA: MEDICAL INFORMATION

- 5. Expands the definition of protected "personal information" to include any information regarding the individual's medical history or condition, medical treatment or diagnosis or genetic information by health care professional.
  - **Medical information NOT just protected by HIPAA.**

16

HB 904 AMENDMENT TO NCITPA: BREACH DETERMINATION

- 6. Expands the definition of "security breach" to include any incident of unauthorized access to unencrypted records **or** acquisition. Now notice duties triggered if information just accessed.
- Current version: A security breach is defined as "an incident of unauthorized access to **and** acquisition of unencrypted and unredacted records or data containing personal information or illegal use of the personal information has occurred or is reasonably likely to occur or that creates a material risk upon to a consumer."
- **Any determination that illegal use has not occurred, or no material risk shall be documented and maintained for at least 3 years.**

17

NCITPA; BROAD DEFINITION OF "BUSINESS"

"A sole proprietorship, partnership, corporation, association or other group however organized and **whether or not organized to operate at a profit.** The term includes a financial institution organized, chartered or holding a license or authorization certificate under the laws of this state and any other state, the United States or any other country, or the parent or the subsidiary of any such financial institution. Businesses shall not include any government or government or subdivision or agency."

18

NCITPA: SOCIAL SECURITY NUMBER PROTECTION

A business may not intentionally:

1. Communicate or otherwise make available to the public an individual's social security number.
2. Intentionally print or imbed an individual's social security number on any card required for the individual to access products or services provided by the person or entity.
3. Require an individual to transmit his or her social security number over the internet unless the connection is secure or the social security number is encrypted.
4. Require an individual to use his or her social security number to access an internet website unless a password or unique personal identification number or other authentication device is also required to access the internet website

19

OTHER PROTECTIONS FOR SOCIAL SECURITY NUMBERS

"A business covered by this section **shall** make reasonable efforts to cooperate, through systems testing or other means, to ensure that the requirements of this Article are implemented."

- Important – this creates a duty for all businesses to safeguard and protect social security numbers and have systems testing to make sure they comply with this section.
- A violation of this section is an unfair and deceptive trade practice which could subject your business to treble damages and an award of attorney's fees

20

PROTECTED PERSONAL INFORMATION

1. Includes a person's first name and/or first initial and last name in combination with any of the following:
   a. Social security number or employer taxpayer identification number
   b. Driver's license, state identification card or passport number
   c. Checking account number
   d. Savings account number
   e. Credit card and debit card number
   f. PIN numbers
   g. Electronic identification numbers, email or address, ~~internet account numbers~~ or internet identification names
   h. Digital signatures
   i. Any other numbers or information that can be used to access a person's financial resources
   j. Biometric data
   k. Fingerprints
   l. Passwords
   m. Parent's legal surname prior to marriage
   n. Health Insurance policy number, subscriber identification number, or any other unique identifier used by a health insurer or payer to identity the person.
   o. Any information regarding the individual's medical history or condition, medical treatment or diagnosis, or genetic information, by a health care professional.

21

NCITPA: OBLIGATIONS REGARDING THE DESTRUCTION OF RECORDS THAT CONTAIN PERSONAL INFORMATION

Any business that conducts business in North Carolina and maintains personal information of a resident of North Carolina must take reasonable measures to protect against unauthorized access to or use of the information in connection with or after its disposal.

22

PROTECTING DATA DURING DISPOSAL

Reasonable measures for the protection of personal information during disposal include:

1. Implementing and monitoring compliance **with policies and procedures** that require the destruction of papers containing personal information and the erasure of electronic media.
2. Businesses must have written policies relating to the adequate destruction or proper disposal of records containing personal information.
3. This obligation can be met if a business enters a written contract with a third party engaged in the business of record destruction. Note, this section does not apply to financial institutions or healthcare facilities subject to HIPAA or consumer reporting agencies, however, these entities are also subject to federal regulations which require the safeguarding and destruction of personal information.

23

BUSINESSES THAT MUST PROTECT CUSTOMER INFORMATION FROM A BREACH

- Any business that owns or licenses personal information of residents of North Carolina or any business that conducts business in North Carolina that owns or licenses personal information in any form (whether computerized, paper, or otherwise) shall provide notice to the affected person that there has been a security breach following discovery or notification of the breach.
- If business does not own data, but maintains the data, the business must notify the owner of the data (i.e. vendors).
- NOTE: NCITPA can apply to NC residents **AND** residents of other states if the business conducts business in NC.

24

OTHER STATES DATA PROTECTION AND BREACH NOTIFICATION STATUTES

- **No national uniform law**: Have to look at all states and countries where your clients reside.
- All states now have a data protection, breach notification law.
- Laws are similar but key differences, including timing and contents of breach notification, definition of breach and affirmative duties to protect data.
- Define protected personal information differently.
- Various credit monitoring requirements.

25

OTHER STATES DATA PRIVACY LAWS

- Other states' statutes may apply to businesses in NC that maintain personal information of residents of that state and have different obligations: Some examples:
  - 1. **Florida and Colorado:** Have a 30-day breach notification deadline to individuals (current shortest period).
  - 2. **Vermont:** 14-day notice from breach discovery to Attorney General.
  - 3. **California Consumer Privacy Act (CCPA):** Goes into effect January 1, 2020. Generally allows residents to know what data being collected and how the data is being used. Discourages monetization of data and promotes transparency in data collection.
  - 4. **EU General Data Protection Regulation (GDPR):** Provides for greater data protection, breach notification, access and control of individual's personal information. Requires notice of breach to regulatory agency within **72 hours.**

26

POTENTIAL LIABILITY FOR FAILURE TO COMPLY WITH THE APPLICABLE STATUTES

1. Customers can bring a lawsuit for actual damages suffered and a violation of the NCITPA is a violation of the NC Unfair and Deceptive Trade Practices Act subject to treble damages.
2. Regulatory investigations and fines (i.e., the North Carolina Attorney General or the FTC)
3. Loss of goodwill and business reputation.
4. Loss of customers

27

WAYS TO PROTECT YOUR BUSINESS FROM LIABILITY

1. **Develop policies regarding the safeguarding and destruction of company property that includes customer's protected information**, with some of the following provisions:
   - Employees shall not, directly or indirectly misappropriate, divulge, disclose, make use of, or in any way communicate to any person, firm, or corporation any Personal Information except in furtherance of employee's duties as an employee of the Company.
   - **Breach response plan including team members, types of data maintained, where data maintained, and whose data is maintained, i.e. where individuals for whom you have data reside.**
   - Employees shall not remove any Personal Information from any premises of Company, except in furtherance of employee's duties as an employee of Company.
   - Employees shall not download or otherwise electronically store any Personal Information on any personal computer, phone or other personal electronic device.
   - Employees shall not intentionally or knowingly publish or broadcast any Personal Information on any public forum, including the internet, social media or any electronic medium of any kind.

28

WAYS TO PROTECT YOUR BUSINESS FROM LIABILITY

- Employees disclosing Personal Information inconsistent with this policy, whether the release is inadvertent, will be subject to discipline, up to and including termination.
- Employees shall not intentionally communicate or otherwise make available to the general public an individual's social security number.
- Employees shall take all reasonable measures to protect against unauthorized access to or use of Personal Information in connection with or after the disposal of documents or other records that contain Personal Information
- Notify a supervisor and/or manager of any unauthorized or inadvertent disclosure of Personal Information.
- **If a suspected breach occurs, perform a risk assessment, document findings and maintain for at least three years.**

29

WAYS TO PROTECT YOUR BUSINESS FROM LIABILITY CONTINUED…

2. General Computer hygiene:
    a. Keep up to date anti-virus and anti-malware software on all computers.
    b. Require complex passwords and regularly change passwords.
    c. Do not download or update a program unless you are specifically looking for it.
    d. Do not open any suspicious link without consulting with your IT department.
    e. Do not visit unknown websites unless they are work related and you have a high degree of confidence in the website.
    f. Ensure there is a mechanism to erase data remotely from portable electronic devices that contain customers' personal information.

30

WAYS TO PROTECT YOUR BUSINESS FROM LIABILITY CONTINUED…

3.**Regularly Train employees** about:

1. Policies regarding the protection and proper disposal of personal information.
2. Breach response plan.
3. Use of all laptops, phones and any other portable electronic devices that contain personal information and have proper passwords and/or encryption.
4. Computer hygiene practices.

31

WAYS TO PROTECT YOUR BUSINESS FROM LIABILITY CONTINUED

32

WAYS TO PROTECT YOUR BUSINESS FROM LIABILITY CONTINUED…

- 4. ALWAYS verify any phone or email requests for personal information with the person who appears to be requesting the information before sending.
- 5. PURCHASE A CYBER LIABILITY INSURANCE POLICY

33

CYBER LIABILITY INSURANCE POLICIES

If your business handles protected information, get a cyber liability policy.

Cyber liability now likely excluded from CGL policies and contain numerous definitions of types of cyber liability risks.

Clients may request Certificates of Insurance (COI) with respect to cyber liability policies.

34

WAYS TO PROTECT YOUR BUSINESS FROM LIABILITY AFTER A SUSPECTED BREACH

Conduct	Conduct a risk assessment, contact breach response team including outside IT consultant and counsel to determine if breach occurred and how to mitigate any damage and close any security gaps.
Document	Document the risk assessment.
Notify	If a breach has occurred, notify the affected individuals and attorney general's offices within the applicable statutory deadlines, for all state statutes that apply.
Offer	Offer credit monitoring services.
Notify	Notify Law enforcement.

35

RESPONDING TO A SUBPOENA

36

STATE OF NORTH CAROLINA

File No.

_____ County

In The General Court Of Justice
☐ District ☐ Superior Court Division

Additional File Numbers

VERSUS

SUBPOENA

G.S. 1A-1, Rule 45; 8-59, -61, -63; 15A-801, -802

Party Requesting Subpoena
☐ State/Plaintiff ☐ Defendant

NOTE TO PARTIES NOT REPRESENTED BY COUNSEL: Subpoenas may be produced at your request, but must be signed and issued by the office of the Clerk of Superior Court, or by a magistrate or judge.

TO

Name And Address Of Person Subpoenaed

Alternate Address

Telephone No.

Telephone No.

YOU ARE COMMANDED TO: (check all that apply)

☐ appear and testify, in the above entitled action, before the court at the place, date and time indicated below.
☐ appear and testify, in the above entitled action, at a deposition at the place, date and time indicated below.
☐ produce and permit inspection and copying of the following items, at the place, date and time indicated below.
☐ See attached list. (List here if space sufficient)

Name And Location Of Court/Place Of Deposition/Place To Produce

Date To Appear/Produce, Until Released

Time To Appear/Produce, Until Released ☐ AM ☐ PM

Date

Name And Address Of Applicant Or Applicant's Attorney

Signature

☐ Deputy CSC ☐ Assistant CSC ☐ Clerk Of Superior Court
☐ Magistrate ☐ Attorney/DA ☐ District Court Judge
☐ Superior Court Judge

Telephone No. Of Applicant Or Applicant's Attorney

RETURN OF SERVICE

37

DUTY OF CONFIDENTIALITY

- 21 NCAC 8N .0205(a)
  - A CPA shall not disclose any confidential information obtained in the course of employment or a professional engagement except with the consent of the employer or client.
- Accountant-client privilege **is not** recognized in NC
  - State v. Agnew, 294 N.C. 382, 394, 241 S.E.2d 684, 692 (1978)

38

EXCEPTIONS – DUTY OF CONFIDENTIALITY

- 21 NCAC 8N .0205(b)(1)-(7)
  - Reporting obligations pertaining to Section .0400 (Attest Services);
  - CPA's compliance **with an order of court or a validly issued subpoena by the Board of CPA Examiners**;
  - Responding to inquiry made by the AICPA Ethics Division or Trial Board, by a duly constituted investigative or disciplinary body of a state CPA society, or under state statutes;

39

EXCEPTIONS – DUTY OF CONFIDENTIALITY CONTINUED

- Disclosure of confidential client information necessary for the peer review process or for any quality review program;
- Assisting the Board in enforcing the accountancy statutes and rules;
- Disclosure of confidential information to state or federal authorities when the CPA concludes in good faith based upon professional judgment that a crime is being or is likely to be committed; or
- **Disclosure of confidential information when such disclosure is required by state or federal laws or regulations**.

40

CIVIL SUBPOENA

- Civil action
- Testimony and/or production of documents
- Ensure subpoena is valid, if any question have a judge decide after filing a motion to quash the subpoena.

41

N.C.G.S. § 75-28: UNAUTHORIZED DISCLOSURE OF TAX INFORMATION

- Except in accordance **with proper judicial order**, or as otherwise provided by law, it shall be unlawful for any person, firm or corporation employed or engaged to prepare, or who or which prepares or undertakes to prepare, for any other person or taxpayer any tax form, report or return, to disclose, divulge or make known in any manner or use for any purpose or in any manner other than in the preparation of such form, report or return, without the express consent of the taxpayer or person for whom the form or return is prepared, the name or address of the taxpayer or such other person, the amount of income, income tax or other taxes, or any other information shown on or included in such form, report or return, or any information which may be or may have been furnished by the taxpayer or such other person to the preparer of such form, report or return or to the person, firm or corporation so employed or engaged.
- Nothing in this section shall be construed to prohibit the examination of any person, books, papers, records or other data in accordance with the authority provided in G.S. 105-258.
- Any person, firm or corporation, or any officer, agent, clerk, employee, or former officer or employee, of any firm or corporation engaged or formerly engaged in the preparation of tax forms, reports or returns for others, whether acting for himself or as agent for such corporation, who or which **shall violate the provisions of this section shall be guilty of a Class 1 misdemeanor.**
- Similar federal civil and criminal penalties for certain disclosures of financial institution records.

42

GRAND JURY SUBPOENA

- Criminal action
- Testimony and/or or production of documents
- Rule 6(e)(6) Federal Rules of Criminal Procedure
  - Records, orders, and **subpoenas** relating to grand-jury proceedings must be kept under seal to the extent and if necessary, to prevent the unauthorized disclosure of a matter occurring before a grand jury.
- Knowing violation of Rule 6 FRCRP may be punished as contempt of court.

43

DEALING WITH A SUBPOENA

- Do not ignore it.
- Contact your client.
  - Possible exception if it is a grand jury subpoena.
- Determine who signed it.
- Contact us to determine proper course of action.
- Contact your insurer-could provide coverage if given notice per policy.

44

RECENT DECISIONS

45

HEAD
V.
GOULD KILLIAN CPA GROUP, P.A., ET AL.

- 2018 NC Supreme Court decision
  - Reversed to trial court
- Client sued CPA and CPA's firm asserting claims for professional negligence and fraudulent concealment

46

IN RE JOHNSON

- 2018 NC Supreme Court decision
  - Upheld NC Board of CPA Examiners' disciplinary actions
- CPA failed to comply with required auditing standards
- CPA failed to fulfill the terms of a peer review contract
- CPA failed to timely respond to the Board and its staff during an investigation

47

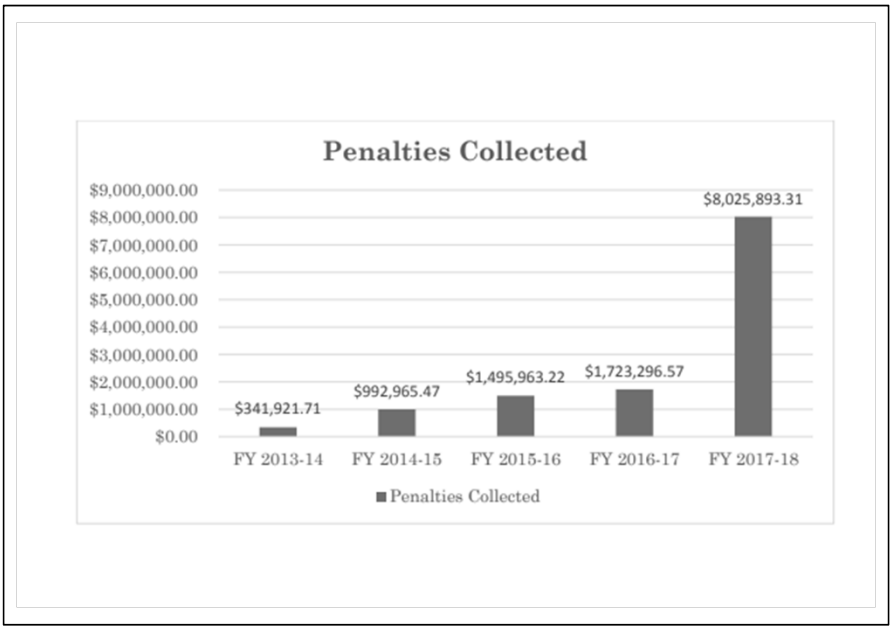
ENFORCEMENT OF WORKERS COMPENSATION LAWS

48

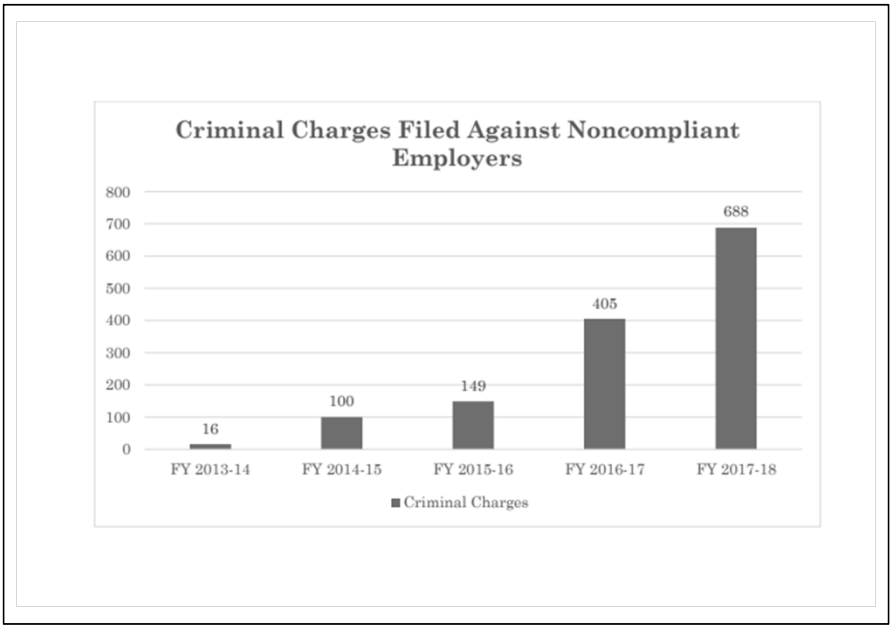
NC WORKERS COMPENSATION ACT

- Enforced by the NC Industrial Commission
- Requires employers who have three or more employees, including corporate officers, to have workers' compensation insurance
- Remedy for a first time violation

49



50



51

EMPLOYEE FAIR CLASSIFICATION ACT

- Effective December 31, 2017
- Employers misclassifying employees as independent contractors
- Employee Classification Section of the NC Industrial Commission
- Information shared with other state agencies
  - Department of Labor, Division of Employment Security, Industrial Commission's Compliance and Fraud Investigative Division, Department of Revenue, and federal agencies

52

QUESTIONS?

Robert N. Young

Trisha L. Barfield

Carruthers & Roth, P.A.

Email: rny@crlaw.com, tlb@crlaw.com

Phone: (336) 478-1131, (336) 478-1176

53