DATA BREACH NOTIFICATION CHECKLIST

This checklist is in reference to The Florida Information Protection Act's (FIPA) data breach notification requirements. Please read the applicable law in its entirety to determine when and how notice is required and which agencies, if any, to notify. You may wish to seek legal counsel for further guidance. The Florida Bar cannot provide legal advice.

- **Read and understand** the Florida Information Protection Act (FIPA), § 501.171, Fla. Stat.
  - Requires that covered entities, governmental entities, or third-party agents take reasonable measures to protect and secure data in electronic form containing personal information.
  - Imposes data breach notification requirements on covered entities.

- **Are you a "covered entity?"** Includes 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.
    - Personal information is defined as:
      - An individual's first name or initial and last name in combination with one or more of the following data elements for that individual:
        - A social security number;
        - 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;
        - A financial account number or credit or debit card number, in combination with any required security code, access code, or password that is necessary to permit access to an individual's financial account;
        - Any information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional; or
        - An individual's health insurance policy number or subscriber identification number and any unique identifier used by a health insurer to identify the individual.
      - 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.
      - Excludes information about an individual that has been made publicly available by a federal, state, or local governmental entity.
      - *Excludes 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.*
  - **No, I am not an entity that acquires, maintains, stores, or uses personal information.** FIPA doesn't apply to you. You may STOP reading.

- **Yes, I am an entity that acquires, maintains, stores, or uses personal information.** FIPA applies to you. Continue reading.

- **Have you had a data breach?** "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.
  - **No, there has been no unauthorized access of data in electronic form containing personal information.** Nothing to notify (yet). You may STOP reading.
  - **Yes, there has been unauthorized access of data in electronic form containing personal information.** Continue reading.

- **Will the breach likely result in identity theft or financial harm? Consult with law enforcement.** 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.*
  - **No, law enforcement determined that the breach has NOT and will NOT likely result in identity theft or other financial harm.** Nothing to notify (yet). You may STOP reading.
  - **Yes, law enforcement determined that the breach HAS or WILL likely result in identity theft or other financial harm.** Continue reading.

- **REQUIRED: Notice to individuals whose personal information has 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 an authorized delay or waiver. Read § 501.171 (4), Fla. Stat. for details.
  - **Notice may be sent via mail or email.** Read § 501.171 (4), Fla. Stat. for details.
  - **The notice to an individual with respect to a breach of security shall include, at a minimum:**
    - The date, estimated date, or estimated date range of the breach of security.
    - A description of the personal information that was accessed or reasonably believed to have been accessed as a part of the breach of security.
    - 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.

- **Has the breach affected 1,000 or more individuals at a single time?**
  - **No, the breach has not affected 1,000 or more individuals at a single time.** Move on to the next orange bullet point.
  - **Yes, the breach has affected 1,000 or more individuals at a single time.** Continue reading.
    - **REQUIRED: Notice to all consumer 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.

- **Has the breach affected 500 or more individuals in Florida?**
  - **No, the breach has not affected 500 or more individuals in Florida.** Move on to the next orange bullet point.
  - **Yes, the breach has affected 500 or more individuals in Florida.** Continue reading.
    - **REQUIRED: Notice to the Department of Legal Affairs.** 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.
      - **Written notice must include:**
        - A synopsis of the events surrounding the breach at the time notice is provided.
        - The number of individuals in this state who were or potentially have been affected by the breach.
        - 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.
        - A copy of the notice required under subsection (4) or an explanation of the other actions taken pursuant to subsection (4).
        - 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.

- **This checklist is not exhaustive. Read FIPA in its entirety!** Here it is, again: § 501.171, Fla. Stat.
  - This checklist is in reference to FIPA's data breach notification requirements. FIPA, for example, also includes requirements for the disposal of customer records containing personal information. Read § 501.171 (8), Fla. Stat. for details.
  - You may still be subject to the other data privacy laws and protections that exist at both the state and federal levels.

- **Practical tips:**
  - Just in case you forgot, read and understand FIPA: § 501.171, Fla. Stat.
  - Consider hiring independent forensic investigators/IT specialists to help you determine the source and scope of the breach.
  - SEEK LEGAL COUNSEL with privacy and data security expertise. They can advise you on other federal and state laws that may be implicated by a breach. The Florida Bar cannot provide legal advice.
  - Visit the FTC's Data Breach Response: A Guide for Business for valuable information.
  - Anticipate questions that clients/the public will ask. Then, put top tier questions and clear, plain-language answers on your website where they are easy to find.
    - Don't publicly share information that might put clients at further risk.
  - ENCRYPT YOUR DATA. FIPA excludes encrypted, secured, or modified information that removes elements that personally identify an individual, or that otherwise renders the information unusable, from its definition of personal information. You are not a "covered entity" if you do not acquire, maintain, store, or use personal information.
  - Download the sample Data Breach Notification letter from our Document Library.
    - Note: The sample letter cannot possibly cover all practice areas or breach scenarios. You will need to customize it to accurately represent your specific circumstances.
    - Don't withhold key details that might help clients protect themselves and their information.
  - Free CLE: watch Cybersecurity for the Everyday Lawyer for important cybersecurity information.
  - Consider preemptively contacting The Florida Bar's Attorney Consumer Assistance Program Hotline at 866-352-0707 to report the incident.