Detailed Outline – What is SPII and What Notice is Required under Alabama's Data Breach Act?

I. What is SPII? Data in
   a. Electronic form for
   b. Alabama resident, that includes
   c. 1st name or initial,
   d. And last name,
   e. in combination with one or more of the following for the same resident: (all id. numbers must be the entire number)
      i. Id Number:
         1. Social security number
         2. Tax identification number
         3. Driver's license number
         4. State-issued identification card number
         5. Passport number
         6. Military identification number
         7. Other unique identification number issued on a government document used to verify the identity of a specific individual
      ii. Financial Information:
         1. Financial account number
            a. Bank account number
            b. Credit card number
            c. Debit card number
         2. In combination with one of following that is necessary to access the financial account or conduct a transaction that will credit or debit the financial account
            a. Security code
            b. Access code
            c. Password
            d. Expiration date
            e. PIN
      iii. Medical Information – any information on
         1. Medical history
         2. Mental or physical condition, **or**
         3. Medical treatment or diagnosis by a health care professional
      iv. Health Insurance
         1. Health insurance policy number or subscriber identification number, **and**
         2. Unique identifier used by a health insurer to identify the person
      v. Certain Online Account Access – Account Information below that gives access to online accounts affiliated with the covered entity where account is reasonably likely to contain or is used to obtain above sensitive personally identifying information
         1. User name or email address,
         2. **and**

a. password, or
b. security question and answer

II. Breakdown of Notice
   a. To the Individual
      i. *Timeframe*: expeditiously and without unreasonable delay taking into account the time necessary for an investigation
         1. upon determining the two findings above are present, but no later than 45 days from the discovery of the breach
      ii. *Address on Notice*:
         1. *Direct Notice* - to the mailing or emailing address of the individual, whichever is on file. If an entity has both, consider sending to both addresses.
         2. *Substitute Notice*
            a. *When* - At times, direct notice may not be feasible due to excessive cost (either in relation to the entity's resources or simply over $500,000), when over 100,000 affected individuals, or a lack of contact information for the individuals.
            b. *What is it* – Substitute notice must include both
               i. Conspicuous notice on the entity's website, if one, for 30 days; and
               ii. Notice in print and broadcast media in areas where affected individuals reside
            c. *Alternatives* - the Alabama Attorney General can approve an alternative method of substitute notice
      iii. *Contents of Notice*: Must include all of the following
         1. *Date* – either the date, estimated date or estimated date range of the breach
         2. *Description* –
            a. of the SPII acquired;
            b. of the actions taken to restore security and confidentiality of the information taken; and
            c. of steps the individual can take to protect from identity theft
         3. *Contact Information* – of the entity for the individual to contact the entity about the breach
      iv. *Exception*: Notice should not be sent if the entity receives written request from Federal or state law enforcement to delay sending the notice.
   b. To the Attorney General
      i. *Only when* – This notice is only required when the entity must send notice to over 1000 individuals.
      ii. *Timeframe* – In general, notice to the Attorney General should be sent quickly, but similar to notice to the individuals, must be sent:
         1. *Within 45 days* – of receiving notice of the breach from a third-party agent
         2. *Immediately* – upon determining that the two findings are present (a. breach occurred, and b. reasonably likely to cause substantial harm)

iii. *Contents of Notice* – The notice must contain all of the following:
    1. *Synopsis of Events*
    2. *Number of Individuals Affected* – estimate if necessary
    3. *Free Services being Offered and Instructions*
    4. *Contact Person at the Entity* – include name, address, phone number and email
iv. *Updates* – allowed but not required
v. *Confidential* – Information marked confidential will not be subject to the Open Records Act

c. To all consumer reporting agencies compiling files on consumers nationwide
    i. *Only When* - notice is sent to the Attorney General
    ii. *Timeframe* – without unreasonable delay
    iii. *Contents of Notice* – timing, distribution and content of other notices