

Act to Strengthen Identity Theft Protections

Rep. Jason Saine and Attorney General Josh Stein

Prevents Breaches

- ✓ **Updates what constitutes a security breach.** Any incident of unauthorized access to *or* acquisition of someone's personal information is a breach. The new definition will now include Ransomware attacks – these are when personal information is accessed but is not necessarily acquired. As a result, the breached organization must notify both the affected consumer(s) and the Attorney General's office. This will empower the affected person and the Attorney General's Office to determine the risk of harm – not the breached organization.
- ✓ **Tighter data protection.** Imposes a duty for a business that owns or licenses personal information to implement and maintain reasonable security procedures and practices – appropriate to the nature of personal information – to protect the personal information from a security breach. Additionally, the definition of protected information is updated to include medical information and insurance account numbers.

Increases Consumer Protection After a Breach

- ✓ **Quicker consumer notification.** When a consumer's personal information has been compromised by a security breach, the entity that was breached must notify the affected consumer and the Attorney General's office within 15 days. This quick notification will allow consumers to freeze their credit across all major credit reporting agencies and take other preventative measures to prevent identity theft before it occurs.
- ✓ **Credit freeze.** Consumers will be able to place and lift a credit freeze on their credit report at any time, for free. A credit freeze will prohibit a thief from using a consumer's stolen information to open any new credit line under the consumer's name. Credit agencies will also be required to put in place a simple, one-stop shop for freezing and unfreezing a consumer's credit reports across all major consumer reporting agencies without any additional action by the consumer.
- ✓ **Credit reports.** Consumers who have suffered a breach will have access to three free credit reports from each consumer reporting agency that compiles and maintains files on consumers on a nationwide basis.
- ✓ **Credit monitoring.** If a security breach occurs at a consumer reporting agency, like Equifax, that agency will have to provide five years of free credit monitoring to affected consumers.
- ✓ **Clarifies penalties.** A business that suffers a breach and failed to maintain reasonable security procedures will have committed a violation of the Unfair and Deceptive Trade Practices Act and each person affected by the breach represents a separate and distinct violation of the law.

Provides Greater Consumer Control

- ✓ **Consent.** A company seeking to obtain or use a consumer's credit report or credit score will need the consumer's permission and must disclose the reason for seeking access to the information.
- ✓ **Right to request information.** A consumer will have the right to request from the consumer reporting agency a listing of the information maintained on him or herself (both credit related and non-credit related information), its source, and a list of any person or entity to which it was disclosed.