Summary: Public Hearings on Consumer Protection and Data Security

House Committee on Commerce and Economic Development

In the Fall of 2017 the House Committee on Commerce and Economic Development held four public hearings concerning consumer protection and data security in the wake of the Equifax security breach. The meetings were held on Thursday, November 9 in the towns of Springfield and Barton, and on Tuesday, November 14 in Manchester and Burlington. Members of House Commerce were joined at one or more venues by other members of the House and Senate, as well as the Office the Vermont Attorney General and the Department of Financial Regulation.

Chairman Botzow opened each of the four hearings with opening remarks concerning the dual purposes of the hearings: (1) to provide information to the public concerning the Equifax data breach and advise Vermonters on steps to safeguard their personal information; and (2) to provide a forum for the public to give feedback to the General Assembly about their experiences with data security and identity theft and offer ideas to improve consumer protection.

Following these remarks, Legislative Counsel David Hall provided an overview of the federal and State legal framework that governs the regulation, use, disclosure, disposal, and protection of consumer personal and financial information. At the federal level, Counsel Hall discussed the applicability of the FTC Act, the Gramm-Leach-Bliley Act, and the Fair Credit Reporting Act on businesses, financial institutions, and consumer reporting agencies. He further discussed applicable Vermont statutes and rules, which in many cases go beyond the minimum standards set in federal law and required more stringent data security requirements for businesses operating in Vermont, including the Vermont Consumer Protection Act, the Vermont Fair Credit Reporting Act, the "opt-in" rules adopted by the Department of Financial Regulation, and the Vermont Security Breach Notice Act.

Next, representatives from the Vermont Attorney General's Office (see Appendix A below), the AG's Consumer Assistance Program at the University of Vermont, and the Department of Financial Regulation, provided an overview of the specific steps those offices have taken since the Equifax breach to respond to consumers' concerns. The speakers addressed the regulatory role and authority within State government to protect Vermont consumers; the role of "data brokers" and other businesses in collecting and using personal and financial information; and common issues concerning scams, data security, and identity theft.

Regulators gave the following guidance for Vermont consumers:

(1) Contact the Consumer Assistance Program at consumer.vermont.gov or 800-649-2424.

(2) Place a "credit freeze" on your credit file with each of the three national consumer reporting agencies (Equifax, Experian, and Transunion).

(3) Monitor your credit information and financial accounts on a regular basis.

(4) File your annual tax returns as early as possible.

Following these presentations by the legislative and executive branch officials, members of the public and press had the opportunity to share their thoughts and concerns, which included the following:

(1) Consumers should not bear the burden of paying for a credit freeze and monitoring their credit files, accounts, etc., when the risk to personal and financial security was caused by Equifax's failure to safeguard sensitive data in its possession.

(2) Consumers typically do not have a direct business relationship with the consumer reporting agencies and should be able to exert control over how those agencies acquire, maintain, and share personal and confidential information.

(3) Consumers are having a difficult time communicating with the consumer reporting agencies, are not certain whether their information is at risk, and should generally have a much easier experience when attempting to safeguard their data.

(4) A credit freeze should be free and automatic; the agencies should be responsible for ensuring continued access to credit information without burdening consumers.

(5) Vermont should regulate data brokers and other businesses to protect personal and confidential information.

(6) There is significant tension between wanting and needing to use technology for personal and business transactions, and wanting and needing sufficient data security measures to protect personal and confidential information.

(7) Scams and financial harm occur frequently, including by telephone scams and through telephone number spoofing; computer hacking; and identity theft caused by a failure of government entities and private businesses to safeguard information contained on hardware or in computer networks.

(8) The companies should be required to create a victim relief fund.

(9) We should explore a "public option" to replace the consumer reporting agencies and the current system.

(10) We should explore the European Union model of data security requirements, privacy standards, and penalty structure.

Possible legislative and regulatory action steps to improve consumer protection include the following:

(1) Eliminate all fees to freeze and thaw consumer credit files.

(2) Require companies that experience data breaches to provide free, no-strings-attached, ongoing credit monitoring.

(3) Require a one-step freeze and thaw process, whereby consumers need contact only one consumer reporting agency and that agency communicates the request to the others.

(4) Enhance the security of the freeze process by requiring a more sophisticated PIN number or some sort of multi-factor authentication to freeze and thaw credit files.

(5) Require all businesses that possess personally identifiable information to implement an information security program, similar to the Massachusetts standard.

(6) Require cybersecurity insurance.

(7) Create a "Chief Security Officer" position and a Cyber Security Council within State government.

(8) Establish that a breach of the Security Breach Notice Act, and a failure to maintain an information security program, are violations of the Consumer Protection Act.

(9) Regulate data brokers.

(10) Adopt standards similar to the proposed FCC rule regulating data security and internet service providers and telecommunications companies.

Appendix A: Information from the Vermont Attorney General's Office

The Attorney General was pleased to participate in public hearings established by Vermont lawmakers in four communities (Springfield, Barton, Manchester, and Burlington) around the state on November 9th and 14th. We know that Vermonters are angry, frustrated, and concerned about this data breach. The Attorney General shares those sentiments.

Here is what we know:

- Equifax is one of three major credit reporting agencies that track and rate the financial history of consumers (the other two are Experian and TransUnion); it gets consumer data from banks, credit card companies, retailers and lenders

- Between May and July of 2017, the company experienced a major security breach exposing sensitive information of nearly 143 million Americans – and 240,000 Vermonters

- The information accessed by an unauthorized party includes: names, social security numbers, addresses, and in some cases credit card numbers and drivers' license numbers.

- Reports indicate that Equifax discovered the breach on July 29, 2017. It reported the breach to the public on September 7, 2017.

What the Attorney General is doing:

- We are investigating this matter and Vermonters can expect we will continue to enforce Vermont's consumer protection and data breach laws.

- The Attorney General is taking consumer complaints at our Consumer Assistance Program: **800-649-2424**, or "**consumer.vermont.gov**" (do not enter "www"). We will continue to update our website with updates and information as we become aware of new information.

- We continue to aggressively pursue education and outreach opportunities to help businesses avoid data breach and to help Vermonters protect themselves against identity theft

- We also issued a **Scam Alert** in conjunction with the Department of Public Safety directly to about 15,000 Vermonters to warn them. Vermonters may sign up for Scam Alerts here: https://www.uvm.edu/consumer/forms/sign-scam-alerts. The Scam Alert system is a new function of the VT-Alert system of the Department of Public Safety developed in consultation with the Attorney General. When there are spikes in scam activity, or new scams happening, the Attorney General may contact enrolled Vermonters directly by voicemail, text, or email -

whatever preference is designated by the user. This is one way to let folks know ahead of time when suspicious activity is occurring. Our hope is that Vermonters will help share the information with family and friends by word of mouth, social media, and other methods.

- More information is available at: http://blog.uvm.edu/cap/identity-theft-and-information-on-the-equifax-data-security-breach/

What Vermonters can do:

- Don't panic. Be vigilant.

- Check credit reports for any unauthorized activity. You can do that by going to any one of the three credit reporting agencies and get one free credit report per year. Or, you can go to www.annualcreditreport.com.

- Monitor your bank accounts and credit card statements for any unusual or unauthorized activity.

- You may request credit monitoring services, or a credit freeze depending on how concerned you are about whether you were affected and/or if you think you may be the victim of identity theft.

- Go to our website for updates and information as this situation develops. Just type "consumer.vermont.gov" into your web browser (again, don't include the "www"). Just go to: "consumer.vermont.gov"

What Equifax is doing:

- Equifax is encouraging concerned consumers to go to its website to see if they may be affected.

- Equifax is also offering one year of free credit monitoring through a product it calls "TrustedID".

- We cannot vouch for the efficacy or accuracy of Equifax' website or services.

- What we can do is reassure Vermonters that they are not waiving their rights if they go there. Many consumers expressed concerns about their website "terms of use" that indicated consumers might waive their legal rights or be bound to arbitration if they used the site.

The Attorney General immediately demanded answers and resolution of these questions from Equifax' General Counsel and can now assure Vermonters of the following:

1) No waiver terms or binding arbitration will be imposed on consumers who go to the Equifax website to learn if they are affected by this data breach.

2) No waiver terms or binding arbitration will be imposed on consumers who enroll in the one year of free identity theft protection and credit file monitoring ("TrustedID") being offered as a result of this breach.

3) No waiver terms or binding arbitration will be imposed on consumers who request a credit report freeze as a result of this breach.

4) Equifax also provides an "opt out" of the standard waiver or binding arbitration clause related to its terms of use for other products and services beyond items 1-3 above. Consumers may do so by writing within 30 days to: Equifax Consumer Services LLC, Attn.: Arbitration Opt-Out, P.O. Box 105496, Atlanta, GA 30348. Be sure to include your name, address, and Equifax User ID, as well as a clear statement that you do not wish to resolve disputes with Equifax through arbitration.

Ensuring the safety and security of Vermonters' sensitive data following this debacle is a top priority for the Attorney General and his staff. We will continue to enforce our consumer protection laws and work to get answers for Vermont consumers as we learn more about this developing situation.

Vermonters can also learn more about our office's recommendations with respect to data brokers generally (in partnership with the Department of Financial Regulation) by reading our report, here: http://ago.vermont.gov/assets/files/Consumer/Data_Broker_Working_Group/2017-12-15%20Data%20Broker%20Working%20Group%20Report.pdf

Appendix B: Protection of Consumer Information - Overview

The legal framework that regulates the collection, use, disclosure, disposal, and security of personal and financial consumer information is complicated. There is no single law addressing these diverse aspects of protecting consumer information; rather, multiple layers of federal and state law regulate consumer protection and data security in different manners and contexts. Enforcement falls under the jurisdiction of many different federal and state entities, including the Consumer Financial Protection Bureau, the Federal Trade Commission, the functional federal regulators for various financial institutions, e.g., FDIC, NCUA, Federal Reserve Board, etc., and state insurance regulators. To the extent permitted under federal law, states may also have additional provisions enforced by Attorneys General, state financial regulators, or other public agencies and departments.

Overarching the host of federal laws is the Federal Trade Commission Act. This law prohibits unfair methods of competition and unfair or deceptive acts or practices in or affecting commerce. Whereas other federal laws apply to specific types of businesses or in particular legal contexts, the FTC Act and enforcement action by the Federal Trade Commission more broadly applies to business practices across industries that cause harm to consumers. In the past several years, the FTC has brought enforcement proceedings under the Act and other laws against companies involved in prominent data breaches. The FTC typically charges these companies with unfair and deceptive trade practices—whether because the company misrepresented the scope or effectiveness of its data security program or consumer protection practices, or because the company failed to comply with its own policies.

In addition to the FTC Act, two major suites of federal statutes and regulations address the use and protection of consumer financial information: The first suite, the Fair Credit Reporting Act and associated rules, applies to consumer reporting agencies, consumer reports, and persons who use or furnish consumer credit information. In general, the act requires that: (1) consumer reporting agencies provide access to consumer credit information, take steps to ensure the accuracy of that information, and observe requirements designed to mitigate identity theft; (2) consumer reports include correct information and are available only for specific permitted purposes; (3) users observe statutory requirements for permissible, legitimate use of a report and certify to the use; and (4) furnishers of consumer credit information supply correct information and observe requirements to facilitate disputes and correction of inaccurate information and mitigate identity theft.

The second suite, the Financial Services Modernization Act, also referred to as Gramm-Leach-Bliley, and its associated rules, applies broadly to financial institutions, which includes both banking institutions and also other businesses that are significantly engaged in providing financial products or services—a category that includes, for example, check-cashing businesses; payday lenders; mortgage brokers; nonbank lenders; personal property or real estate appraisers; professional tax preparers courier services; retailers that extend credit; automobile dealers that lease vehicles for more than 90 days; and any other business that is significantly engaged in a financial activity described in section 4(k) of the Bank Holding Company Act of 1956. A financial institution subject to GLB must provide notice of its privacy policies and is limited in its ability to disclose nonpublic personal information. Additionally, the "Safeguards Rules" adopted under authority of GLB require financial institutions to implement an information security program that includes administrative, technical, and physical safeguards to ensure the security and confidentiality of, and prevent unauthorized access to, customer records and information. Of particular

significance, the GLB requirements also apply to persons with whom a financial institution shares nonpublic personal information, including consumer reporting agencies.

Another regulatory layer of federal statutes and rules impose requirements on the collection, use, and disclosure of consumer information in specific legal contexts. For example, the Children's Online Privacy Protection Act relates specifically to websites that collect information from children under age 13. The Driver's Privacy Protection Act limits disclosures of personal information by State departments of motor vehicles. The Family Educational Rights and Privacy Act restricts the disclosure of educational records. The Federal Privacy Act imposes extensive requirements on the collection and use of personal information by agencies of the federal government. Finally, the Health Insurance Portability and Accountability Act imposes duties and limits relating to personal health information.

The final layer of federal law creates crimes for the collection or misuse of personal information. For instance, the Computer Fraud and Abuse act prohibits unauthorized access to computers and trafficking in passwords. The Electronic Communications Privacy Act prohibits the unauthorized interception, use, or disclosure of wire, oral, or electronic communications, and unauthorized access to stored electronic records. The Federal Identity Theft and Assumption Deterrence Act makes it a federal crime to produce or possess false identity documents and to use another person's identity to commit a crime. The Video Privacy Protection Act prohibits the unauthorized disclosure of consumer information relating to video rentals, sales, and viewing history, such as on internet sites like Facebook and Netflix.

In addition to these federal laws, states generally have authority to impose additional requirements, which in many cases are more stringent than federal law. For example, 13 states have laws that apply to any business that has access to consumer personal information and require the business to implement a data security program similar to the GLB Act. Almost every state, including Vermont, has a data breach notification law, which requires notice to consumers (and often to the state Attorney General) when a data breach occurs.

Like many other states, Vermont has scores of state laws across most legal subject areas that seek to limit the disclosure of personal or confidential information by government-related activities. Specific Vermont laws mandate the protection of, and limit the use and disclosure of, social security numbers; require businesses to take reasonable steps to destroy records with personal information; limit a consumer's liability for unauthorized use of a credit card; and create a State law crime of identity theft.

Vermont law goes beyond the requirements of federal law in many areas. For example, with respect to financial institutions, insurance companies, and securities professionals, Vermont not only requires regular notices of privacy policies, but also requires Vermont consumers to "opt in" to allow those companies to disclose personal information to nonaffiliated third parties. Vermont also imposes on these entities the duty to have an information security program similar to the GLB Act.

Finally, with respect to credit reports and credit reporting agencies, Vermont limits the use of credit information for employment purposes, and with limited exceptions, requires written consent from the consumer before a person can obtain his or her credit report. Like many states, Vermont allows a consumer to place a "security freeze" on his or her credit file, imposes certain state-specific notice requirements for consumers, caps the amount and applicability of certain fees, and mandates one free annual credit report from each consumer reporting agency.