June 13, 2017

The Honorable Patrick Morrisey
Attorney General of West Virginia
Attn: Brett Tubbs
State Capitol Building 1, Rm. E-26
1900 Kanahwa Blvd. East,
Charleston, WV 25305

Email: brett.w.tubbs@wvago.gov

Re: Efforts Against Identity Theft

Dear Attorney General Morrisey:

This letter is in response to a letter from Attorney General Morrissey of May 15, 2017, requesting the assistance of the American Financial Services Association ("AFSA")[1] in fighting identity theft in West Virginia. Your letter was addressed to Franc Lee, Chairman of AFSA; I am replying on behalf of AFSA. Thank you so much for reaching out to us on this important issue.

AFSA shares your concerns about identity theft and is committed to working with government, regulators, and law enforcement to ensure that personal information, particularly financial information, is protected from exploitation by criminals. As data are increasingly stored in electronic formats, ensuring the safety and security of consumer information is a priority and a challenge for many industries, including financial services. Hackers and other criminals are becoming increasingly sophisticated in their efforts to defeat data security measures, and it is expected that these techniques will continue to evolve as time goes on.

High-profile data breaches involving the theft of consumer payments data have been especially troubling over the last few years. Some AFSA members have been at the forefront of the effort to ensure more secure payments, and the adoption of the new EMV standard for payment cards (the so-called "chip" card) is evidence of progress. EMV cards make it nearly impossible for criminals to clone credit, debit or prepaid cards, removing an incentive for identity theft. Complementary to this, technologies such as Tokenization, which replaces consumer data stored in merchant systems with electronic "tokens" that are worthless to criminals, and Point-to-Point Encryption (P2PE), which protects consumer data in transit, for instance, at the point-of sale which is often vulnerable to Malware, are creating an environment in which it is ever more difficult for criminals to access usable consumer data.

[1] Founded in 1916, the American Financial Services Association (AFSA), based in Washington, D.C., is the primary trade association for the consumer credit industry, protecting access to credit and consumer choice. AFSA members provide consumers with many kinds of credit, including direct and indirect vehicle financing, traditional installment loans, mortgages, payment cards, and retail sales finance. AFSA members do not provide payday or vehicle title loans.

Of course, AFSA members are subject to a number of important federal laws aimed at protecting consumer data. The Gramm-Leach-Bliley Act (GLBA) sets forth requirements regarding the treatment of nonpublic personal consumer information by financial institutions. Under GLBA, financial institutions are prohibited from disclosing this information to third parties unless the institution makes the required opt-out disclosures and the consumer has not selected to opt-out of sharing this information.[2] Upon the creation of the Consumer Financial Protection Bureau (CFPB), authority over the majority of the provisions of the GLBA, with the exception of regulation related to certain motor vehicle dealer companies, as well as securities and futures businesses, was delegated to the agency, which issued revised rules that outline specific notices, privacy standards, and limitations on disclosure of nonpublic consumer information, including the prohibition of disclosure to non-affiliated third parties for marketing purposes without providing an opt-out.[3]

The Privacy of Consumer Financial Information Rule (Privacy Rule or Regulation P)[4] carries out major provisions of the GLBA. The Privacy Rule requires the disclosure of clear and conspicuous privacy notices to both customers and consumers who are not customers with information about the financial institution's privacy policies and practices. These notices contain opt-out provisions providing enough time for the consumer to choose to opt-out before financial institutions share their nonpublic information, which information is collected and which is disclosed, and to whom that information is disclosed, any disclosures required by the Fair Credit Reporting Act (FCRA), and confidentiality disclosures. The Privacy Rule also governs how notices must be delivered to consumers, as well as limitations on the reuse and re-disclosure of nonpublic information with nonaffiliated third parties.[5]

The FTC has also issued the Safeguards Rule as part of the GLBA, requiring financial institutions under the authority of the FTC to maintain certain protections in order to keep consumer's financial information secure. The rule applies to all businesses engaging in the sale of financial products or services, including payday lenders, check cashers, non-bank lenders, mortgage brokers, real estate appraisers, courier services, credit reporting agencies, ATM operators and tax preparers. These institutions are required to develop a written information security plan that assesses risks and implements and monitors a safeguards program.[6]

---

[2] The Federal Deposit Insurance Corporation, *Gramm-Leach-Bliley Act (Privacy of Consumer Financial Information*, at https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=15&cad=rja&uact=8&sqi=2&ved=0ahUKEwjms4-M_O_SAhUo0oMKHYvaB7EQFghsMA4&url=https%3A%2F%2Fwww.fdic.gov%2Fregulations%2Fcompliance%2Fmanual%2F8%2FVIII-1.1.pdf&usg=AFQjCNF5hLqxe2egvtsMj1gKMvw94gfRZw&sig2=F5iMYSlpNptYV2Gwt7ySMw (June 2016).

[3] *Id*.

[4] 16 C.F.R. § 313.

[5] Federal Trade Commission, *How To Comply with the Privacy of Consumer Financial Information Rule of the Gramm-Leach-Bliley Act*, at https://www.ftc.gov/tips-advice/business-center/guidance/how-comply-privacy-consumer-financial-information-rule-gramm (July 2002).

[6] Federal Trade Commission, *Financial Institutions and Customer Information: Complying with the Safeguards Rule*, at https://www.ftc.gov/tips-advice/business-center/guidance/financial-institutions-customer-information-complying (April 2006).

While GLBA is primarily concerned with disclosure of nonpublic information to nonaffiliated third parties, the FCRA governs disclosure of personal information among affiliates, including Consumer Report information and information for marketing purposes. The FCRA and Regulation V allow for sharing transaction and experience information among affiliates, but Consumer Report information may not be shared without first giving the consumer an opportunity to opt out. The FCRA also prohibits an affiliate from using nonpublic information for marketing purposes unless it has been conspicuously disclosed to the consumer the information may be used for solicitations and the consumer has been given an opportunity to opt out.

Beyond GLBA and FCRA, AFSA members also follow the FTC Red Flags Rule[7], which requires financial institutions to implement an Identity Theft Prevention Program. It requires companies to identify "red flags" – which are indications of possible identity theft. As part of this program, a financial institution is required to update the Red Flags Program as it learns of new identity theft tactics. The FTC's Disposal Rule[8] is another important privacy regulation. The Disposal Rule provides: "Any person who maintains or otherwise possesses consumer information for a business purpose must properly dispose of such information by taking reasonable measures to protect against unauthorized access to or use of the information in connection with its disposal." This would require, for example, shredding paper documents containing personal information.

In addition to compliance with these important data-protection regulations, AFSA members recognize the importance of working directly with law enforcement to bring criminals to justice and to develop new and ever more sophisticated ways to thwart them.

AFSA's federal compliance team ensure that AFSA members have access to information and resources relating to data security and the dangers of identity theft. AFSA recently published a fact sheet on *Synthetic Identity Theft* (whereby real consumer data is used to create fake credit files), for that purpose. AFSA University, AFSA's compliance training program for members which has over 22,000 AFSA member company employees enrolled, also contains modules on federal privacy law, including modules specifically focused on identity theft.

AFSA members are committed to protecting their customers' information and follow industry standard practices to maintain the security and confidentiality of consumer information, such as clean desk policies, document shredding policies, use of secure file rooms and secure servers, virus protection software and encryption technology.

As you know, fraudsters' tactics are constantly evolving. It seems like every month brings news of new threats and breaches. AFSA members invest tremendous resources to combatting cyberthreats to and within their organizations. AFSA as an association engages on this issue constantly. On May 25, 2017, AFSA members met jointly with the National Association of Consumer Credit Administrators (NACCA), and brought in a speaker to address the newest threats, common myths, case examples, and practical advice by the Co-Founder of Defense

[7] 16 C.F.R. § 681.
[8] 16 C.F.R. § 682.3.

Storm, a cybersecurity management platform. The previous day AFSA members met with a former agent of the U.S. Secret Service, who shared information on the latest threats he's observed now in private practice.

AFSA is very happy to work with the West Virginia Attorney General's office in this important area. If you have any questions or would like to discuss this further, please do not hesitate to contact me at 952-922-6500 or dfagre@afsamail.org.

Sincerely,

Danielle Fagre Arlowe
Senior Vice President
American Financial Services Association
919 Eighteenth Street, NW, Suite 300
Washington, DC 20006-5517