

ELLEN F. ROSENBLUM

ATTORNEY GENERAL



FREDERICK M. BOSS

DEPUTY ATTORNEY GENERAL

DEPARTMENT OF JUSTICE

Justice Building  
1162 Court Street NE  
Salem, Oregon 97301-4096  
Telephone: (503) 378-6002

February 11, 2019

**TRANSMITTED ELECTRONICALLY**

Donald S. Clark, Secretary of the Commission  
Federal Trade Commission  
Office of the Secretary  
600 Pennsylvania Avenue, NW  
Suite CC-5610 (Annex B)  
Washington, DC 20580

Re: Identity Theft Rules, 16 C.F.R. Part 681  
Project No. 188402

Dear Secretary Clark:

The Attorneys General of Oregon, Alaska, California, Colorado, Connecticut, Delaware, District of Columbia, Hawaii,<sup>1</sup> Illinois, Iowa, Kentucky, Maine, Maryland, Massachusetts, Michigan, Minnesota, Mississippi, Nebraska, Nevada, New Jersey, New Mexico, North Carolina, Oklahoma, Pennsylvania, Rhode Island, Tennessee, Utah, Vermont, Virginia, Washington, and Wisconsin ("State Attorneys General") submit the following Comment in response to the request for public comment on whether any modifications should be made to the Red Flags Rule and the Card Issuers Rule that were issued by the Federal Trade Commission ("Commission") in 2007.

Our offices receive numerous reports of data breaches each month. Through no fault of individual consumers, their personal information, including names, addresses, phone numbers, online account credentials, Social Security numbers, drivers' license numbers, passport numbers, financial account information, credit/debit card information, biometric information, and health information are regularly stolen and made available for purchase on the Dark Web. Even if a specific breach compromises only certain pieces of personal information, information obtained from different breaches is aggregated and used for identity theft purposes. Individual consumers

---

<sup>1</sup> Hawaii is being represented on this matter by its Office of Consumer Protection, an agency which is not part of the state Attorney General's Office, but which is statutorily authorized to undertake consumer protection functions, including legal representation of the State of Hawaii.

have no way of knowing which pieces of their stolen information are being used by whom and at what time to open new accounts, including credit cards, utility accounts and for vehicle purchases. Furthermore, because so many data breaches have occurred, identity thieves are able to amalgamate consumer data with exact accuracy to cause financial harm.

The Identity Theft Rules (“the Rules”), known as the “Red Flags Rule” and the “Card Issuers Rule,” appropriately place the burden on certain entities to detect, prevent and mitigate identity theft. Only these entities have the ability to stop a fraudulent account from being opened at their own place of business or to notify a consumer of a change of address in conjunction with a request for an additional or replacement card, which is a strong indicator that the account may have been taken over by an identity thief.

We see evidence of many businesses taking their responsibilities under the Rules seriously through the course of our investigations – particularly in investigations that are unrelated to data security. For example, in investigations that relate to motor vehicle dealers’ sales practices, we see documentation regarding compliance with the Red Flags Rule.

We strongly believe there is a continued need for the Rules, as repealing the Rules would leave consumers more vulnerable to identity theft. Financial institutions and creditors are uniquely positioned to help detect, deter and prevent identity theft. Identity theft is widespread and causes serious harm to individuals, businesses and the economy.<sup>2</sup> For example, one report found that, in 2017 alone, 16.7 million U.S. consumers were victims of identity fraud and fraudsters stole \$16.8 billion from U.S. consumers.<sup>3</sup> Preventing and stopping harm resulting from identity theft requires everyone, from businesses to individuals to government, to do their part.

The Rules complement the laws of states that have enacted laws requiring entities to develop, implement and maintain reasonable safeguards to protect the security, confidentiality and integrity of personal information.<sup>4</sup> For example, in Oregon, these reasonable safeguards must include administrative, technical and physical safeguards.<sup>5</sup> Similarly, in Massachusetts, entities must develop, implement and maintain a written comprehensive information security program that contains administrative, technical and physical safeguards.<sup>6</sup> A repeal of the Rules would place consumers at greater risk of identity theft, especially consumers in states that have not enacted such laws.

---

<sup>2</sup> See, e.g., Consumer Sentinel Network Data Book 2017, [https://www.ftc.gov/system/files/documents/reports/consumer-sentinel-network-data-book-2017/consumer\\_sentinel\\_data\\_book\\_2017.pdf](https://www.ftc.gov/system/files/documents/reports/consumer-sentinel-network-data-book-2017/consumer_sentinel_data_book_2017.pdf) (last visited Feb. 8, 2019), Identity Theft Resource Center, <https://www.idtheftcenter.org/surveys-studys> (last visited Feb. 8, 2019), Insurance Information Institute, <https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime> (last visited Feb. 8, 2019).

<sup>3</sup> Javelin Strategy & Research, <https://www.javelinstrategy.com/press-release/identity-fraud-hits-all-time-high-167-million-us-victims-2017-according-new-javelin> (last visited Feb. 8, 2019).

<sup>4</sup> See, e.g., Cal. Civil Code § 1798.81.5; Del. C. § 12B-100, *et seq.*; Illinois Personal Information Protection Act, 815 ILCS 530/1, *et seq.*; KRS 61.932 and KRS 365.732; Md. Code Ann., Com. Law § 14-3503 (2013 Repl. Vol and 2018 Supp.); Title 201 of the Code Massachusetts Regulations (CMR), section 17.00, *et seq.*; Neb. Rev. Stat. § 87-808; NRS 603A.010, *et seq.*; ORS 646A.622; R.I. Gen. Laws Chapter 11-49.3; Utah Code §13-44-201; Vermont Consumer Protection Act, 9 V.S.A. § 2453 and 9 V.S.A. § 2447.

<sup>5</sup> ORS 646A.622.

<sup>6</sup> 201 CMR 17.03(1).

Because the Rules are so flexible, they have generally kept up with changes in technology. However, we request some modifications to ensure their continued relevance. One modification to 16 C.F.R. §681.2 would account for changes in email addresses, cell phone numbers or other means of communication, since identity thieves will change other contact information at the same time as changing a mailing address to try to prevent detection by the true account holder.<sup>7</sup> Specifically, if an email address or cell phone number has been changed at around the same time that a physical address was changed, notification to the cardholder of a change of address request under 16 C.F.R. §681.2(c)(1)(i)(B) should be made at both the old and new email addresses or both the old and new phone numbers.

Another requested modification is to amend Appendix A to highlight current best practices. In the Supplement A to Appendix A, under the heading “Suspicious Personal Identifying Information,” example number #18 states that it would be suspicious if a person opening a covered account or a customer cannot provide authenticating information beyond that which generally would be available from a wallet or consumer report. While true, we are concerned that the example implies that knowledge-based authentication, by itself, is an acceptable form of authentication. There is growing concern that, in today’s world, identity thieves can now overcome knowledge-based authentication questions, either because the questions are weak or the answers are readily available online or previously compromised from a data breach.<sup>8</sup> In a well-known example, a student in Tennessee successfully reset the password for Vice-Presidential candidate Sarah Palin’s email account and gained access to its contents by using a simple Google search to obtain Palin’s birthdate, zip code and where Palin met her spouse.

With information gleaned from data breaches or publicly available on social media sites, identity thieves can be better than consumers at answering knowledge-based authentication questions because they have the data in front of them, whereas consumers need to try to recollect events that happened years prior. Thus, even if a person can provide some authenticating information, identity thieves may not be sufficiently screened from opening or accessing an account. Therefore, we would delete example number #18 and instead encourage more modern forms of authentication, such as multi-factor authentication.<sup>9</sup>

Similarly, in the Supplement A to Appendix A, under the heading “Unusual Use Of, or Suspicious Activity Related to, the Covered Account” example number #21 lists examples of ways that an account may be used in a manner that is not consistent with established patterns of activity on the account. There are now many different ways that identity thieves try to use stolen information or impersonate another individual to open a new account or take over an existing

---

<sup>7</sup> Stolen Passwords Fuel Cardless ATM Fraud, Brian Krebs, (Jan. 5, 2017) <https://krebsonsecurity.com/2017/01/stolen-passwords-fuel-cardless-atm-fraud> (last visited Feb. 8, 2019).

<sup>8</sup> Everybody Knows: How Knowledge-Based Authentication Died, Mike Baukes, (Jan. 22, 2018) <https://www.forbes.com/sites/forbestechcouncil/2018/01/22/everybody-knows-how-knowledge-based-authentication-died/#37656ab54eee> (last visited Feb. 8, 2019); Hack of data brokers highlights weakness of knowledge-based authentication, Tony Bradley, (Sept. 27, 2013) <https://www.csoonline.com/article/2137128/access-control/hack-of-data-brokers-highlights-weakness-of-knowledge-based-authentication.html> (last visited Feb. 8, 2019).

<sup>9</sup> U.S. Dept. of Commerce, National Institute of Standards and Technology, <https://www.nist.gov/itl/tig/back-basics-multi-factor-authentication> (last visited Feb. 8, 2019).

account to perpetrate fraud.<sup>10</sup> To keep pace with the ingenuity of identity thieves, we suggest modifying this section to also include the following examples of suspicious activity related to the use of an account:

- A covered account accessed by new and previously unknown devices based on a user's prior behavior pattern;<sup>11</sup>
- A covered account accessed by new and previously unknown IP addresses based on a user's prior behavior pattern;
- An unauthorized user trying to guess account passwords over several unsuccessful attempts;<sup>12</sup> and
- Foreign IP addresses attempting to access multiple accounts within a close period of time.<sup>13</sup>

The State Attorneys General thank the Federal Trade Commission for the opportunity to provide a Comment to aid in the Commission's review of its rules to prevent identity theft. We appreciate the consideration of our Comment and look forward to continuing to work collaboratively with the Commission to protect consumers.

Sincerely,



ELLEN F. ROSENBLUM  
OREGON ATTORNEY GENERAL



KEVIN G. CLARKSON  
ALASKA ATTORNEY GENERAL



XAVIER BECERRA  
CALIFORNIA ATTORNEY GENERAL



PHILIP J. WEISER  
COLORADO ATTORNEY GENERAL



WILLIAM TONG  
CONNECTICUT ATTORNEY GENERAL



KATHLEEN JENNINGS  
DELAWARE ATTORNEY GENERAL

---

<sup>10</sup> A new form of ID theft: account takeover, Sabri Ben-Achour, (Aug. 21, 2017) <https://www.marketplace.org/2017/08/21/economy/new-form-id-theft-account-takeover> (last visited Feb. 8, 2019); Identity Thief sentenced for using a new form of fraud "Synthetic Identities", (April 28, 2017) <https://www.justice.gov/usao-ndga/pr/identity-thief-sentenced-using-new-form-fraud-synthetic-identities> (last visited Feb. 8, 2019).

<sup>11</sup> Your mobile phone account could be hijacked by an identity thief, Lorrie Cranor, (June 7, 2016) <https://www.ftc.gov/news-events/blogs/techftc/2016/06/your-mobile-phone-account-could-be-hijacked-identity-thief> (last visited Feb. 8, 2019).

<sup>12</sup> Beware of older cyber attacks: Footprinting and brute force attacks are still in use, Scott Craig, (April 2016) <https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SEL03093USEN> (last visited Feb. 8, 2019).

<sup>13</sup> Sift Science, Inc., <https://siftscience.com/sift-edu/prevent-fraud/device-ip-analysis> (last visited Feb. 8, 2019).



KARL A. RACINE  
DISTRICT OF COLUMBIA ATTORNEY GENERAL



STEPHEN H. LEVINS  
EXECUTIVE DIRECTOR OF HAWAII OFFICE OF  
CONSUMER PROTECTION



KWAME RAOUL  
ILLINOIS ATTORNEY GENERAL



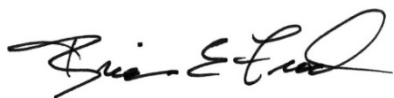
TOM MILLER  
IOWA ATTORNEY GENERAL



ANDY BESHEAR  
KENTUCKY ATTORNEY GENERAL



AARON M. FREY  
MAINE ATTORNEY GENERAL



BRIAN E. FROSH  
MARYLAND ATTORNEY GENERAL



MAURA HEALEY  
MASSACHUSETTS ATTORNEY GENERAL



DANA NESSEL  
MICHIGAN ATTORNEY GENERAL



KEITH ELLISON  
MINNESOTA ATTORNEY GENERAL



JIM HOOD  
MISSISSIPPI ATTORNEY GENERAL



DOUGLAS PETERSON  
NEBRASKA ATTORNEY GENERAL



AARON D. FORD  
NEVADA ATTORNEY GENERAL



GURBIR S. GREWAL  
NEW JERSEY ATTORNEY GENERAL



HECTOR BALDERAS  
NEW MEXICO ATTORNEY GENERAL



JOSHUA H. STEIN  
NORTH CAROLINA ATTORNEY GENERAL



MIKE HUNTER  
OKLAHOMA ATTORNEY GENERAL



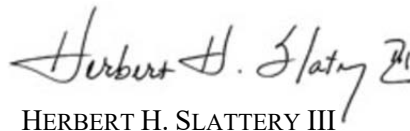
JOSH SHAPIRO  
PENNSYLVANIA ATTORNEY GENERAL

February 11, 2019

Page 6



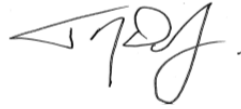
PETER F. NERONHA  
RHODE ISLAND ATTORNEY GENERAL



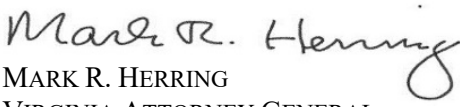
HERBERT H. SLATTERY III  
TENNESSEE ATTORNEY GENERAL



SEAN D. REYES  
UTAH ATTORNEY GENERAL



THOMAS J. DONOVAN, JR.  
VERMONT ATTORNEY GENERAL



MARK R. HERRING  
VIRGINIA ATTORNEY GENERAL



BOB FERGUSON  
WASHINGTON ATTORNEY GENERAL



JOSHUA L. KAUL  
WISCONSIN ATTORNEY GENERAL

DM9313395