Keynote Remarks of Commissioner Terrell McSweeny[1]
Future of Authentication Policy Forum
October 13, 2017
Washington D.C.

Thank you Jeremy, for that kind introduction, and thank you very much for inviting me to be here today. This forum could not be more timely. Current events–including the recent breach at Equifax, and the revelation last week that all three billion Yahoo! email accounts in existence during 2013 were affected by a previously disclosed hack–have forced consumers, industry, law enforcers, and policymakers to all take a long, hard look at what more we should be doing to protect personal data.

Cybersecurity is a collaborative effort, and all of us have important roles to play. The FTC is pursuing several approaches in this area simultaneously. The one that gets the most attention is our law enforcement work, where we bring cases against companies that either don't live up to the promises they make about privacy and data security, or that fail to take reasonable measures to protect consumers' personal information. Our law enforcement cases have involved companies in a wide variety of industries–including brick and mortar retailers, social media companies, hardware manufacturers, and even Uber and the online dating site Ashley Madison.

While vigorous law enforcement is critical to serve as a deterrent and to motivate firms to take data security seriously, this isn't a problem that can be addressed solely through case-by-case enforcement actions after the fact. That's why the FTC is engaged in proactive efforts to prevent data security breaches from occurring in the first place.

These include our extensive efforts on consumer and business education. While education is one of the Commission's core consumer protection priorities generally, it is especially important in the area of data security, where the breathtaking pace at which new technologies are introduced is matched only by the alarming rate at which new security threats are discovered.

For consumers, we provide practical information about how you can reduce your risk of having your data compromised, including how to spot a phishing scam that might deliver malware, the risks of using public wi-fi, and the need to update software and use strong passwords. We also provide extensive resources to consumers who have been the victim of identity theft. Our website, identitytheft.gov–which is also available in Spanish–is a centralized portal where consumers can file a complaint with the FTC and obtain a personalized recovery plan that is customized for their individual needs and circumstances. The site will automatically generate affidavits and pre-fill letters and forms to be sent to credit bureaus, police, debt collectors, and the IRS. We are continuing to work on enhancements to the site to make it even easier and more seamless for consumers.

On the business side, we have devoted considerable efforts to providing concrete, practical guidance that can be implemented by businesses in any industry and of any size. Our

[1] The views expressed in this speech are my own and do not necessarily reflect those of the Commission or any other Commissioner.

Start with Security publication provides important lessons about data security drawn from specific examples in the agency's law enforcement experience.[2] And to make sure that our guidance stays up to date, the FTC just launched a follow-up series of blog posts, called *Stick with Security*, providing current and ongoing guidance.[3]

Also, we convene technical experts, law enforcers, industry representatives, and consumer advocates to discuss evolving technologies and their implications for consumers, including with regard to data security. Topics of recent FTC workshops have included connected cars, identity theft, drones, smart TVs, ransomware, and the Internet of Things. These workshops help focus our efforts on nascent areas of potential concern and sometimes result in the issuance of FTC reports with recommendations to industry or policymakers. The FTC can also leverage our in-house technological research abilities, housed in our Office of Technology Research and Investigation, to conduct original research on the impact of technology on consumers, including with regard to data security.

But let me move to the specific topic of this forum today, which is the need for strong, multi-factor authentication. More than ten years ago, in the spring of 2007, the FTC held a workshop called "Proof Positive: New Directions in ID Authentication," which sought to explore ways to reduce ID theft through the use of enhanced authentication methods.[4] The prominent themes of discussion back then[5] are just as relevant now. First: there is no single "right" way to authenticate individuals, although biometrics, the use of smart cards, and multiple layers of security are all promising technologies. Second: convenience and usability are critical because consumers will reject authentication procedures that are too burdensome. Third: the government can play an important role in this area by encouraging and facilitating the development of better authentication.

On the first point, there has been a substantial amount of innovation in this space during the last decade, and I am optimistic that newer and more reliable authentication methods will continue to be introduced. There is demand for new authentication methods from firms that hold consumers' personal information–who want to avoid breaches and cultivate consumer trust–as well as from consumers themselves, who are increasingly aware of how exposed their personal data has become. At the same time, the need for convenience and usability remains paramount in light of the mind-boggling number of firms with which consumers interact on a regular basis online. For instance, consumers may not embrace the idea of requiring multiple physical tokens to authenticate themselves with multiple firms.

---

[2] Fed. Trade Comm'n, *Start With Security: A Guide for Business* (June 2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.

[3] Thomas B. Pahl, *Stick with Security: Insights into FTC Investigations*, FTC.gov (July 21, 2017), https://www.ftc.gov/news-events/blogs/business-blog/2017/07/stick-security-insights-ftc-investigations.

[4] *See* Press Release, Fed. Trade Comm'n, *FTC To Host Identity Authentication Workshop* (Feb. 21, 2007), https://www.ftc.gov/news-events/press-releases/2007/02/ftc-host-identity-authentication-workshop; Fed. Trade Comm'n, *Proof Positive: New Directions for ID Authentication* (Apr. 23-24, 2007), https://www.ftc.gov/news-events/events-calendar/2007/04/proof-positive-new-directions-id-authentication.

[5] *See Prepared Statement Of The Federal Trade Commission Before The Subcommittee On Social Security Of The House Committee On Ways And Means on Protecting the Privacy of the Social Security Number from Identity Theft* (Jun. 21, 2007), https://www.ftc.gov/sites/default/files/documents/public_statements/prepared-statement-federal-trade-commission-protecting-privacy-social-security-number-identity-theft/p065409socsectest.pdf.

The Commission has explicitly promoted the use of multi-factor authentication, as is clear in our education materials to both consumers and businesses. We advise consumers to use multi-factor authentication when it is offered, and we have expressly advised firms that possess sensitive data to use multiple authentication techniques–in addition to requiring strong passwords–to combat credential stuffing attacks and other online assaults. Examples might be a one-time verification code texted to a consumer's smartphone, a physical token that generates random numbers, or a USB security key.

Likewise, our law enforcement efforts underscore the need for multi-factor authentication in certain circumstances. In our recent case against TaxSlayer,[6] we alleged that the company failed to maintain reasonable security safeguards as required until Gramm-Leach-Bliley[7], which applies to firms providing financial products or services. Our complaint describes how the company fell victim to a successful list validation attack, where attackers used lists of stolen login credentials to attempt to access accounts across multiple sites, knowing that consumers often reuse their user name and password combinations.

As a company in the business of preparing tax returns, TaxSlayer was in possession of extremely sensitive information about its customers, including their Social Security numbers, income, financial assets, tax payments, bank account numbers, and payment card numbers. We alleged that as a result of the list validation attack, hackers gained full access to more than 8,800 TaxSlayer online accounts, and in some cases committed tax ID theft–filing fraudulent tax returns and collecting fabricated tax refunds. Tax ID theft causes tremendous headaches and substantial harm to its victims, including significant delays of legitimate tax refunds they are owed.

In our complaint against TaxSlayer, we alleged that the list validation attack began on October 10, 2015, and stopped on December 21, 2015–the day that the company implemented multi-factor authentication requiring the use of both a password and a code that was sent to customers' email accounts or mobile phones. While the complaint alleged the company suffered from multiple security lapses–including failure to require strong passwords, failure to have a written information security program, and failure to conduct a risk assessment–it is telling that the day when the company began requiring multi-factor authentication is the day that they were able to stop the attack.

Our case against Uber specifically called out the company for failing to require multi-factor authentication to access a third-party cloud storage service the company used to store very sensitive rider and driver information, including trip records, geolocation, and images of driver's licenses.[8] The complaint explains how an intruder was able to access sensitive personal information–not encrypted and stored in clear, readable text–belonging to more than 100,000

---

[6] *See* Press Release, Fed. Trade Comm'n, *Operator of Online Tax Preparation Service Agrees to Settle FTC Charges That it Violated Financial Privacy and Security Rules* (Aug. 29, 2017), https://www.ftc.gov/news-events/press-releases/2017/08/operator-online-tax-preparation-service-agrees-settle-ftc-charges.

[7] Financial Services Modernization Act of 1999, Pub. L. No. 106–102, 113 Stat. 1338 (1999).

[8] *See* Press Release, Fed. Trade Comm'n, *Uber Settles FTC Allegations that It Made Deceptive Privacy and Data Security Claims* (Aug. 15, 2017), https://www.ftc.gov/news-events/press-releases/2017/08/uber-settles-ftc-allegations-it-made-deceptive-privacy-data.

Uber drivers. While Uber claimed to provide reasonable security for the personal information it stored–including claims that it was "extra vigilant" and applied "the highest security standards available "–the FTC alleged that the failure to require multi-factor authentication and other lax security practices made these claims untrue.

So I'd like to encourage all of you to keep innovating and keep pushing for more robust and secure methods of authentication. We are getting to the point where passwords may be becoming passé, and given how much of our private information is already available online, I think we need to take a hard look at the role of knowledge-based authentication. Finally, I want to mention that the Commission has repeatedly asked Congress to pass baseline privacy and data security legislation, including requirements for breach notification. I still think that legislation would be extremely helpful in setting out a unified legal framework for data security as opposed to the patchwork of state and industry-specific federal laws that currently apply.

In closing, I think that the interests of industry, consumers, and the FTC are all aligned. We all want our information to be more secure, to increase consumer trust and confidence, and to promote innovation to help consumers realize the many benefits that new technologies and business models have to offer. I look forward to working with all of you to achieve those goals.