Closing Keynote Remarks of Commissioner Terrell McSweeny[1]
Electronic Transactions Association FinTech Policy Forum
September 14, 2017
Washington, D.C.

Thank you, Jerry, for that very nice introduction. I also want to thank ETA for inviting me to this terrific event, and for putting together such an informative program of experts on FinTech issues.

I want to start off by addressing the news of the day. While the FTC normally does not comment on ongoing investigations, this morning we confirmed that our staff is investigating the data breach at Equifax. We are making this announcement because of the intense public interest and widespread potential impact of the event. As a national credit reporting agency, Equifax is the guardian of massive amounts of sensitive information pertaining to much of the U.S. adult population. I cannot make any further comment on the substance or status of our investigation, but I will say that I am personally very concerned about this breach and Equifax's response. It is unacceptable for consumers to disproportionately bear the risk of a massive breach of their information. I am hopeful that this incident will rekindle the Congressional debate not just about data security legislation – but also about privacy and the obligations to consumers of companies that hold massive amounts of sensitive information.

But let me get back to the topic at hand – FinTech. It is easy to get caught up in the excitement and novelty of the many exciting products and services that are being developed in the FinTech space – and believe me, the FTC is excited about them too. Innovations in this industry have the potential to bring real and meaningful benefits to consumers, including those in traditionally underserved populations who might not otherwise have access to certain financial products and services. We want FinTech to flourish. But at the same time, it's important that we not lose sight of basic consumer protection principles.

The FTC's interest in FinTech is the same interest we have in every industry that falls within our jurisdiction. We are here to enforce common-sense, baseline consumer protection principles that have been the law for decades. The primary statute we enforce – Section 5 of the FTC Act – prohibits deceptive and unfair acts and practices. And that straightforward standard applies to all firms in all industries, regardless of the technology they employ or the method they use to reach and serve their customers.

I want to briefly highlight some recent cases that provide concrete examples of how basic consumer protection principles can apply in the FinTech space. In March, we announced that NetSpend agreed to pay $53 million in refunds to consumers to settle a case we filed last year alleging that it made misrepresentations about its prepaid debit cards.[2] I know a physical prepaid card might seem very old school to this crowd, in comparison to the cutting edge financial

[1] The views expressed in this speech are my own and do not necessarily reflect those of the Commission or any other Commissioner.
[2] *See* Press Release, Fed. Trade Comm'n, *NetSpend Settles FTC Charges* (Mar. 31, 2017), https://www.ftc.gov/news-events/press-releases/2017/03/netspend-settles-ftc-charges.

products and services being developed in the FinTech space now. But the allegations we made in our case against NetSpend could also crop up in a case involving any FinTech service, even if it doesn't involve a physical product.

For instance, we alleged that the company misrepresented that NetSpend cards would be ready to use immediately and provide consumers with immediate, instant, same-day access to their funds. We also alleged the company misrepresented that it would provide provisional credits within a certain timeframe for the full amount of account errors claimed by customers.[3]

These are the types of terms that are going to be vitally important to consumers using any sort of FinTech service that gives them the ability to borrow, share, or spend money. Consumers want to know when their funds will be available and what will happen if an error occurs with their account. These terms are material to consumers, and could influence their decision to choose one service over another. Firms must be truthful about the attributes of their products and follow through on their stated policies. Not only does the law require it, but being forthright with consumers is critical to developing consumer trust in new technologies and encouraging their wider adoption.

Likewise, late last year a court imposed a record $1.3 billion judgment on the operators of a payday lending scheme that hit consumers with undisclosed and inflated fees, and engaged in illegal debt collection practices by threatening borrowers with arrest and lawsuits.[4] While the defendants in this case, including AMG Services and racecar driver Scott Tucker, were involved in online payday lending activities that aren't exactly new, the allegations at the heart of the case can apply to any financial service that provides consumer loans. You cannot lie about the terms of loans, such as the interest rate and finance charges. You cannot misrepresent the length of a payment schedule or the total amount that consumers will pay for a loan.

I'd like to point out that the AMG case involved an entity that both lent money and engaged in collection of debts once the loans it made were overdue. I think that the issue of consumer debts arising from FinTech services is one that likely will be the subject of more attention in the future, as these services mature and loans go into the collection phase. While I am not going to get into details here, suffice it to say that there is an entire legal framework around the issue of consumer debt collection and that firms who engage in such activities need to be aware of their legal obligations and the numerous rights consumers have in this area.

Aside from the basic principle that firms must tell the truth to consumers about their products and services, I want to talk about a couple of other cases that illustrate some additional important considerations for the FinTech industry. The first is our recent case against Western Union, which is an example of what obligations a company has to its customers when it knows that its service is being misused. In January, Western Union entered into agreements with the

---

[3] *See* Press Release, Fed. Trade Comm'n, *FTC Charges Prepaid Card Company Deceptively Marketed Reloadable Debit Card* (Nov. 10, 2016), https://www.ftc.gov/news-events/press-releases/2016/11/ftc-charges-prepaid-card-company-deceptively-marketed-reloadable.

[4] *See* Press Release, Fed. Trade Comm'n, *U.S. Court Finds in FTC's Favor and Imposes Record $1.3 Billion Judgment Against Defendants Behind AMG Payday Lending Scheme* (Oct. 4, 2016), https://www.ftc.gov/news-events/press-releases/2016/10/us-court-finds-ftcs-favor-imposes-record-13-billion-judgment.

FTC, the Department of Justice, and two United States Attorneys' Offices to resolve charges that it aided and abetted wire fraud. [5] Western Union agreed to forfeit $586 million as part of these agreements. Again, while money transfer services like Western Union have been around for a very long time, the conduct challenged in this case could apply to any FinTech service that could be used by criminals to obtain payments procured through fraud.

As many of you are no doubt aware, direct money transfer systems such as Western Union and MoneyGram have been favored by scammers in this country because they allow fraudsters to pick up proceeds quickly, conveniently, and often, anonymously. Further, once a payment is sent through Western Union and collected by the recipient, the sender has no recourse to recover those funds – they are gone. This is in contrast to payment methods such as credit cards, where consumers have the ability to dispute fraudulent transactions and may be able to recover their funds.

When you have a system like this – where sending a payment is the functional equivalent of sending cash that is irrecoverable – you have a responsibility to install controls and procedures to ensure that criminals are not using your company to defraud consumers. We alleged that Western Union was aware that its system was being used for fraud-induced money transfers – such as payments from victims of romance scams and grandparent scams – including by Western Union agents in foreign countries who were complicit in these frauds. However, our complaint alleged that the company harmed consumers by failing to take appropriate measures to detect and prevent such fraud-induced transfers, such as terminating agents and locations involved in high levels of fraudulent transactions, or imposing more robust ID requirements to receive money transfers.

If you are setting up a system that allows consumers to send and receive money, you need to think about whether your service can be exploited by criminals and how it can be designed to protect consumers and their funds. Further, if you have knowledge that your service is in fact being used to facilitate fraud, you must take reasonable steps to protect your customers from being victimized.

Of course, any payment system can be utilized by scammers and there is no requirement for perfection – just to take reasonable measures, especially in response to knowledge that harmful practices are taking place. Also, we recognize that there is a tension between the desire to make transactions as quick and frictionless as possible, and the perception that excessive safeguards might just put an unnecessary speedbump in the way. But you cannot simply sacrifice consumer protection in the quest for convenience.

Another important consideration for FinTech companies is the need to safeguard the personal information of their customers. Particularly in the FinTech space, companies are likely to have sensitive consumer information that can be an attractive target for hackers – not just financial account information, but also personal information or detailed consumer profiles that

[5] *See* Press Release, Fed. Trade Comm'n, *Western Union Admits Anti-Money Laundering Violations and Settles Consumer Fraud Charges, Forfeits $586 Million in Settlement with FTC and Justice Department* (Jan. 19, 2017), https://www.ftc.gov/news-events/press-releases/2017/01/western-union-admits-anti-money-laundering-violations-settles.

might have been used as the basis for making a credit decision. This type of information is data that consumers reasonably expect to be protected. And the law requires that companies honor the promises they make about it. Further, specific laws such as the Fair Credit Reporting Act may provide consumers with additional legal rights and protections for data that is used in making credit decisions.

Earlier this summer we announced a case against Blue Global, a lead generator.[6] The company operated websites that collected very sensitive consumer information – including names, dates of birth, Social Security numbers, bank routing and account numbers, and driver's license numbers – ostensibly in order to match up consumers with companies that would offer them payday loans or auto loans on attractive terms. But we alleged that the company simply sold off consumers' data to anyone willing to pay for it.

We alleged this was problematic on a few levels. First, the defendants misrepresented that consumers would be matched up with a lender that would provide them with a low interest rate and favorable terms, and that most loan applications were approved. That wasn't true. But in addition, the defendants actually sold this sensitive information to other companies that weren't even in the business of making consumer loans, when they promised that it would be shared only with trusted lending partners. You cannot collect consumer information for a particular stated purpose and use it for something else.

Moreover, the Blue Global defendants allegedly sold this sensitive consumer information to entities about which they had little or no information – such as what line of business they were in or where they were physically located. This behavior was reckless and put consumers at tremendous risk for misuse of their information, such as identity theft and account fraud. Also, the defendants used a "ping tree" to offer consumer leads to potential buyers in a particular sequence, but transmitted entire, unmasked loan applications to each entity in the ping tree, even if the recipient did not actually purchase the lead or wasn't even involved in consumer lending. Therefore, the defendants indiscriminately exposed sensitive consumer information to many entities that had no legitimate need to access it.

This case is an extreme example, but it offers some important lessons for companies involved in offering financial services with regard to the need to protect consumer data. First, you cannot lie about the policies your company follows with regard to the collection and sharing of consumer information. Second, you have a responsibility to vet the entities with whom you share your customers' information, especially if it's sensitive information that is obviously prone to misuse. Third, you have to set up your business model in a thoughtful way that takes consumer privacy and security seriously, from the start. A company that embraced the concepts of privacy by design and security by design would not have designed the system we saw in this case where entire unmasked loan applications were shared indiscriminately. Consumers deserve careful treatment of their personal information and the law requires that it be handled reasonably.

[6] *See* Press Release, Fed. Trade Comm'n, *FTC Halts Operation That Unlawfully Shared and Sold Consumers' Sensitive Data* (Jul. 5, 2017), https://www.ftc.gov/news-events/press-releases/2017/07/ftc-halts-operation-unlawfully-shared-sold-consumers-sensitive.

One other topic I want to touch on quickly is the intersection of the Internet of Things and FinTech. I know there was a panel on this topic today, and we can all see in the near horizon a world where consumers are routinely making purchases or transferring money through connected devices and appliances – perhaps you'll be able to tell your intelligent personal assistant to pay your babysitter, your smart refrigerator will be able to place an order for groceries, and your connected washing machine will be able to re-order laundry detergent. This is another area where there is an obvious tension between the desire to make transactions convenient and frictionless, and the need to ensure that consumers are protected from unauthorized purchases and charges. And we have seen how these interests can collide – for instance, in cases we've brought against Apple,[7] Amazon,[8] and Google[9] with regard to how they allegedly allowed children to make unauthorized in-app purchases. Here too, there is a basic underlying principle that continues to apply: you cannot charge consumers without their consent. Firms have to design systems – or devices – with adequate safeguards to ensure that consumers are not charged without their permission.

The themes that I've discussed today – the need to accurately disclose costs and fees, to follow through on stated account dispute procedures, to keep consumer privacy and data security at the forefront, to protect bad actors from using your financial platforms for fraud, and to only charge consumers when you have their informed consent – apply to all companies in the FinTech space. They are the same concepts we have been discussing at our most recent FinTech Forums, which gathered stakeholders together to explore issues in peer-to-peer lending, crowdfunding, blockchain, and artificial intelligence. And by the way, I think that crowdfunding, especially for charitable causes, will get more attention in the near future as we will undoubtedly see more crowdfunding campaigns to raise funds for victims of the recent hurricanes in Texas and Florida – including some that are from fraudsters seeking to capitalize on others' generosity.

I hope that you will keep these principles in mind as you continue to develop innovative and exciting new products that will bring real benefits and opportunities to American consumers.

Thank you.

---

[7] *See* Press Release, Fed. Trade Comm'n, *Apple Inc. Will Provide Full Consumer Refunds of At Least $32.5 Million to Settle FTC Complaint It Charged for Kids' In-App Purchases Without Parental Consent* (Jan. 15, 2014), https://www.ftc.gov/news-events/press-releases/2014/01/apple-inc-will-provide-full-consumer-refunds-least-325-million.

[8] *See* Press Release, Fed. Trade Comm'n, *FTC Alleges Amazon Unlawfully Billed Parents for Millions of Dollars in Children's Unauthorized In-App Charges* (Jul. 10, 2014), https://www.ftc.gov/news-events/press-releases/2014/07/ftc-alleges-amazon-unlawfully-billed-parents-millions-dollars.

[9] *See* Press Release, Fed. Trade Comm'n, *Google to Refund Consumers at Least $19 Million to Settle FTC Complaint It Unlawfully Billed Parents for Children's Unauthorized In-App Charges* (Sept. 4, 2014), https://www.ftc.gov/news-events/press-releases/2014/09/google-refund-consumers-least-19-million-settle-ftc-complaint-it.