Electronic Transactions Association FinTech Policy Forum
Washington, DC
September 22, 2016
Opening Remarks of Commissioner Terrell McSweeny[1]

Thank you, Jeff, for that kind introduction. And thanks very much to the ETA for inviting me to be here today, and to all of you for taking the time to attend this forum to discuss the impact of innovative financial technologies – that give consumers new ways to borrow, share, and spend money – on both consumers and the financial services marketplace.

FinTech is a topic of great interest to the FTC. The reason that we are paying such close attention to FinTech is because it intersects with so many different aspects of our consumer protection mission, in some ways that might be less obvious than others. So this morning I want to talk broadly about some of the major consumer protection issues that we hope FinTech companies will keep in mind.

First, I want to underscore that we recognize and appreciate the potentially significant benefits that FinTech has to offer to individual consumers and businesses alike. Increasing access to credit and financial services can be a matter of convenience for some, but for others it can be a life-changing event – opening up pathways for economic opportunity and increased social mobility.

We want to support and encourage the terrific innovation taking place in the FinTech sector. But these innovations cannot come at the expense of strong consumer protections. And if there is one take away I want to leave you with today it is that transparency is absolutely critical to consumers – not just to protect them from harms but also to build their trust in new and emerging technology.

Transparency is also the foundation of the FTC's consumer protection enforcement program. The FTC is charged with the responsibility of protecting consumers from unfair and deceptive acts or practices under Section 5 of our statute. We have a broad mandate with jurisdiction over almost the entire economy. We have the authority to take action against non-depository institutions involved in financial services, such as non-bank lenders and payment processors. In fact, we have an entire Division of attorneys devoted to investigating companies offering financial services such as payday lenders, debt collectors, credit repair firms, auto dealers, and those selling debt relief or mortgage modification services. We've taken enforcement action against companies in all of these industries, including cases relating to crowdfunding, Bitcoin and cryptocurrency mining, and in-app purchases.

The principles underlying the Commission's consumer protection enforcement agenda remain constant, regardless of the industry or the technology involved. That's an important concept to keep in mind as we see businesses transform their business models and methods of offering and delivering products and services. If you're a company within our jurisdiction, the

---

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

same rules of the road apply whether you operate a brick and mortar location where consumers interact with you in person, or if you have a website where consumers access your services online, or if you develop a mobile app to reach consumers.

The most basic rule to keep in mind is that you need to provide complete and accurate information to consumers. For example, in our case involving Bitcoin, we charged an operation selling Bitcoin mining machines with deceiving thousands of consumers about the availability, profitability and newness of the mining machines. Moreover, you cannot charge consumers for services they do not receive. Again, in our Bitcoin case, the company allegedly kept up-front payments event after failing to deliver the mining machines as promised.

You have to tell the truth about the products and services you're offering, including how much they cost, what fees are involved, what payments are required and on what timetable, and what rights consumers have if they have a complaint or a dispute.

For example, in our first crowdfunding case we alleged that a project creator misrepresented how he would use funds raised on Kickstarter. Now, we recognize that not every crowdfunded project will meet its goals – but in this case we alleged the so-called creator raised nearly four times his goal but spent virtually none of the funds raised on the project. Instead he allegedly spent the money on rent, a move, and licenses for a different project altogether.

In addition, when you are finding new ways to charge consumers for things – for example through billing on their mobile phones or through in-app purchases – you cannot charge consumers for purchases they do not authorize.

Finally, when you make promises about how you protect consumers' personal and financial information, or make representations about with whom you will share such information, you have to keep those promises.

And all material information has to be presented in a clear and straightforward manner, not buried in small print or hyperlink disclosures. It's especially important that companies offering novel technologies take the time to educate consumers about products and services that may not work in the same way as older businesses models with which consumers are more familiar.

For instance, many consumers have experience using credit cards and know how to dispute a charge and how to report a stolen card so that they will not be responsible for fraudulent charges. But do consumers know what rights they have if they are using some type of virtual currency or peer-to-peer payment system that is not funded from an existing credit card and they want to dispute a payment or suspect a charge is fraudulent? And does someone who wants to fund a marketplace loan or help crowdfund a project understand the risks that are involved? It's critical that businesses be up front about the risks of their products, along with the benefits.

Under the FTC Act, firms also have a legal responsibility to enact reasonable data security measures to protect consumers' personal information. Especially where sensitive information such as payment card information, bank account numbers, or Social Security numbers are involved, companies need to keep data security at the forefront of their business decisions, not leave it as an afterthought. This concept of "Security by Design," or incorporating security into every aspect of your business from the outset, is critical to reduce the risk of a data breach and legal exposure down the road.

The specific security measures that are appropriate for any particular company depend on the nature of the business and the sensitivity of the information involved. But for companies that want to learn more about what steps they need to take to implement reasonable data security protections, a great place to start is the FTC's *Start with Security* guide. It's specifically aimed at helping businesses learn about potential security vulnerabilities and provides practical guidance on how to address them.

In addition, the FTC is responsible for enforcing several other laws that may apply to FinTech businesses, not just Section 5 of the FTC act. For instance:

- The **Truth in Lending Act (TILA**) requires creditors to make certain written disclosures regarding finance charges and an annual percentage rate, among other things. These requirements also apply to advertisements for credit.

- The **Equal Credit Opportunity Act (ECOA**) prohibits discrimination by creditors on the basis of race, color, religion, national origin, sex, marital status, age, or because someone receives public assistance. It also requires creditors to provide applicants, upon request, with the reasons underlying decisions to deny credit.

- The **Fair Credit Reporting Act (FCRA)** protects information collected in consumer reports used for the purpose of eligibility decisions including the granting of credit. Companies that compile consumer reports – whether they are based on "traditional" factors such as payment history, or non-traditional factors such as social media activity and shopping habits – must take steps to ensure the accuracy of consumer reports and provide consumers with the ability to correct errors. And companies that use consumer reports – such as a lender that obtains a reports from a third party for the purpose of evaluating creditworthiness – must inform consumers when they are denied credit or provided credit on less favorable terms because of information in their consumer report.

- The **Electronic Fund Transfer Act (EFTA)** prohibits companies from debiting consumers' debit cards, or using other electronic fund transfers to debit bank accounts, on a recurring basis without obtaining proper written authorization. EFTA also prohibits requiring consumers to preauthorize electronic withdrawals as a condition of obtaining credit.

- The **Gramm-Leach-Bliley Act (GLB)** applies to "financial institutions," but the types of companies that fall into that category are far broader than just banks – it includes all businesses, regardless of size, that are "significantly engaged" in providing financial products or services, including payday lenders, check-cashing businesses, mortgage brokers, nonbank lenders, and others. Companies that fall under GLB must follow the

Safeguards Rule, which requires them to protect the consumer information they collect by assessing and addressing information security risks, and the **Privacy Rule**, which requires them to tell their customers about their information-sharing practices.

- The **Fair and Accurate Credit Transactions Act of 2003 (FACTA) Disposal Rule** requires that businesses that obtain consumer reports must take appropriate measures to dispose of sensitive information derived from those reports, to prevent unauthorized access or use of such information.

This may seem like an alphabet soup of laws, but it's the same set of regulations that apply to all businesses in the financial sector, not just those employing new technologies. And you can really boil these laws down to some basic themes that I think we can all agree are grounded in common sense.

Be transparent.

Tell consumers upfront about the costs of your products and services and what you do with their personal information.

Don't discriminate when making credit decisions.

Protect consumer personal and financial information.

Don't debit bank accounts without consent.

When you use third-party consumer reports to make credit decisions, those reports should be accurate and you need to tell consumers when you make adverse decisions based upon information in them.

I also want to talk briefly about another topic that comes up often in the context of FinTech, especially when it comes to non-traditional services offering loans to individuals and small businesses. And that is the issue of "Big Data," or analytics based upon large sets of consumer data from a variety of sources – a development that has been made possible by the ubiquitous collection of such data, the plummeting cost of data storage, and powerful new modeling capabilities to analyze data to draw connections and make inferences and predictions.

Big Data has the potential to provide tremendous benefits to individual consumers and society as a whole, for instance in the areas of medicine, education, health, and transportation. Big data can help match products and services more effectively to consumers, including to those in underserved communities. Increasingly, we are also hearing about the use of big data analytics in the financial services arena, where lenders may evaluate creditworthiness based on alternate scoring models, including algorithms that take into account novel data sources such as zip code and social media usage. This is in contrast to the practices of traditional lenders, who would generally rely upon a FICO score to make decisions about offering a mortgage or car loan.

The FTC held a workshop on big data in late 2014, and published a report in January 2016 examining whether certain uses of big data analytics may harm consumers, particularly low-income and underserved populations. It's important to keep in mind that if you are using someone else's proprietary algorithm to evaluate consumers, you are putting your trust into a process that may be completely opaque to you.

We have to be mindful that even processes that appear to be facially neutral may have a disparate impact on certain groups of people, and can end up excluding instead of including underserved groups. An algorithm used to evaluate creditworthiness could have a disparate impact on certain groups for any number of reasons – perhaps the underlying data set used to develop the algorithm includes inaccurate information, unwittingly incorporated institutional biases, or did not include proportionate samples from various demographic groups. All of these factors can perpetuate inequality.

The risk with use of such an algorithm is not just a moral hazard, but a legal one. As I mentioned earlier, the Equal Credit Opportunity Act makes it illegal for creditors to discriminate against consumers based on certain classifications. Credit screening practices that have a disparate impact on protected groups are prohibited unless they further a legitimate business need that cannot reasonably be achieved by other means with less disparate impact.

Before I conclude, I'd like to give a plug to the FTC's series of FinTech forums examining consumer protection issues related to various aspects of financial technology. We held our first event in June on marketplace lending and we will be hosting another forum on Wednesday, October 26, on crowdfunding and peer-to-peer payments. We'll be gathering industry participants, consumer groups, researchers, and government representatives to discuss different business models, explore potential benefits to consumers, and examine consumer protection concerns and laws that may apply. If you're interested in these issues, we hope to see you there.

Like all of you here, the FTC embraces the many opportunities that FinTech has to offer to consumers. However, we are closely monitoring the marketplace to ensure that firms live up to the challenge of ensuring that consumer protection doesn't fall by the wayside. We look forward to working with industry members and stakeholders to make sure that consumer protections keep pace with technological innovation in this area.