REPORT
FINTECH LAW
E-Banking, Payments & Commerce in the Mobile World

Mar/Apr 2015 ■ Volume 18 ■ Issue 2

Disrupting FinTech Law

BY JO ANN S. BAREFOOT[1]

Innovative technology is disrupting consumer financial services, much in the way that similar technologies have reshaped industries like retailing, publishing, music, and taxis in recent years. The scope and fast pace of these shifts will profoundly impact not only the industry, but also the regulatory framework that oversees financial activity. Some of the coming changes will be mold-breaking and difficult to sort into existing boxes of regulatory strategy and structure.

These developments are making it both possible, and necessary, to rethink consumer protection regulation in financial services. Like all innovations, they will generally create both good and bad results, in terms of direct and indirect impacts on consumers and on the businesses that serve them.

Compared to financial services, most of the industries that have undergone technology-driven disruption have been relatively narrow, lightly regulated, and/or subject to comparatively simple regulatory structures. The financial industry is arguably the first highly-regulated sector to enter into a disruptive era. This means that the years ahead will force the industry, policymakers, and FinTech attorneys into challenging and uncharted terrain.

The first section of this article describes the most impactful innovations developing in the FinTech world. The second part explores regulatory implications of these shifts.

Note that the article's conclusions mainly seek to identify crucial topics needing discussion, rather than offering firm predictions and recommendations. No one can confidently predict even how and how fast technology trends will evolve, much less precisely how and when they will impact consumers and providers. Nevertheless, the FinTech legal and regulatory community should be actively exploring them today, given the speed and unprecedented nature of the coming change.

The challenge can be envisioned as a kaleidoscope, in which public policy seeks to regulate a highly complex interplay of industry business models, products, practices, players, and technologies, only to see them shift into whole new forms, and then shift again, and again, leaving regulatory structures and methods no longer aligned with the need. In fact, this is too simple an image, as the kaleidoscope turns symmetrically at a set pace, whereas changes in the financial world will lurch around asymmetrically and will stall and accelerate in different parts of the system in unpredictable ways. Regulating it will be intensely challenging.

CONTINUED ON PAGE 3

Editorial Board

Fintech Law Report
West LegalEdcenter
610 Opperman Drive
Eagan, MN 55123

One Year Subscription ■ 6 Issues ■ $820.00
(ISSN#: XXXX)

CONTINUED FROM PAGE 1

Top Innovation Trends

There are four major technology trends driving disruptive change: mobile payments and payments change overall (including virtual currency); "big data;" artificial intelligence (AI); and, possibly on a slower track, natural voice recognition and response.

All of these developments overlap and are highly intertwined, and each raises complex subissues. *A critical point is that they are all converging*. As their confluence reaches scale, it is likely to create sharp acceleration of change in areas that may have appeared to be evolving gradually in their individual tracks.

Below is a high-level overview of the major shifts underway.

Mobile Services, Payments Innovation, Digital Currency, and Online Business Models

This category includes overlapping developments in mobile financial activity, the effect of cryptocurrencies on payments, and the evolution of the payment function toward invisibility. It also touches on online business models involving more than mobile and payments.

The most critical and transformative change in this category is that mobile payments—the ability to scan a phone at checkout rather than swiping a card or paying cash—are beginning to change the whole consumer financial marketplace.

While "mobile wallets" have been fairly slow to win consumer acceptance, there are signs that the advent of Apple's mobile payment tool, Apple Pay, will create a breakthrough in adoption. Early data indicate rising use of Apple Pay on the iPhone 6, which has enjoyed extraordinary sales since its release last fall. The launch in March of the Apple Watch will add visibility and "buzz" to the mobile field. Already Google and Samsung have expanded their mobile payment initiatives.

The popularization of mobile payments has profound implications that reach far beyond the payments function *per se*. Consumers typically sub-optimize money management for a range of reasons. Many financial products are complex both to select and to use wisely. Budget-making and tracking require effort. Emotional and cultural factors often make it easier to spend than to save. Also, there is normally a timing disconnect between the information available at the moment a person spends money and receipt of status reports like bank account and credit card statements. Furthermore, bank and card statements are typically not integrated. Consumers using multiple kinds of accounts receive only fragmentary information on their spending and saving or investment patterns, unless they undertake significant work to put it all together and keep it up to date.

The mobile phone will bring substantial solutions to all of these problems. Once people start using their phone routinely for payments, they will discover that it can help them manage nearly every aspect of their financial lives. Widening adoption will in turn generate creation of more and more useful consumer tools. Even for people who tend to be passive rather than active in money management, the phone will begin to bring easy, effortless assistance. Mobile devices will begin consolidating financial activity information with unprecedented clarity, completeness, and accessibility—always at people's fingertips—giving millions of consumers easy ways to check on and manage their money.

An important aspect of this is the evolution of personal financial management (PFM) tools. Existing services like Mint.com have been successful with relatively sophisticated users, but have not easily penetrated the mass market. Automatic consolidation of information in the mobile phone will fuel an explosion of PFM innovation that is already well underway among banks and startups. Most PFM focuses initially on simplified tools to manage budgeting, spending, and saving. As discussed below, the availability of these tools in the handy mobile phone will merge with vast advances in the usefulness and personalization of financial coaching driven by expanding big data, machine learning, and voice technology.

The significance of this shift cannot be overstated. It is likely to change fundamental financial habits for the vast majority of people. As discussed below, it will tend to bring a leap forward in consumer empowerment, along with huge new

risks for consumers. Providers will find new opportunities and risks opening up, and innovators will have the potential to achieve rapid, major-scale disruption of traditional business models.

Also, importantly, mobile services can revolutionize the inclusiveness of the financial system. Lower-income people are disproportionately high users of mobile phones, including for financial tasks like bill-paying and shopping for bargains and coupons. In addition, the intrinsically low cost of mobile delivery channels will tend to broaden access. At the same time, advocates and regulators are concerned about adverse effects of growing mobile services on vulnerable lower-income neighborhoods that could face bank branch closures, and on elderly consumers who may not be adept with mobile devices. These issues are discussed further below.

Another critical aspect of mobile services is geolocation (discussed further below). The Global Positioning System (GPS) in our devices, including the phone, will know where we are and what we might want to buy nearby. Consumer advocates fear that people will be manipulated into irresistible, "pushed" offers of nearby bargains, which will raise growing controversy over the appropriate role of government in "protecting people from themselves." Meanwhile, PFM will use geolocation to warn us away from temptation, if we set it to do so.

While mobile innovation is broader than payments, it is also part of a wider set of shifts in the payments space, and in online financial services overall. Many of these include mobile strategies but are not limited to them. Nonbanks, pioneered by PayPal, have built robust businesses in online payments that are person-to-person (P2P). Facebook announced in March that it will enable payments among its users, at no charge, to name just one recent example

Another subtle but critical shift in payments—again, including, but not limited to mobile payments—is a move toward making the payment process invisible to consumers. Industry experts speak of submerging the payment process in the consumer's total "experience," and of "Uberizing" payments, referring to the fact that an Uber ride ends with the customer simply exiting the car—the payment has already been arranged in the background. Technology is also bringing a shift toward radio-based payments that will enable consumers to skip checkout lines entirely, simply walking out of stores after invisible tools have read digital codes on the items they select and automatically handle the payment.

These developments will bring great convenience but will also raise concerns about privacy, data security, and potential behavioral manipulation of consumers. As discussed below, consumer advocates worry that they will tend to foster overspending and debt over-extension, as consumers become less conscious of the costs of what they buy.

Interacting with both mobile growth and payments change is a related proliferation of online-only businesses. While this model has existed for decades in financial services (and has seen extensive failure), it is gaining momentum today due to accelerating mobile and online usage (most banking is now done online), and in response to extensive investment in innovation, some of it sparked by lessons learned in the financial crisis. An important subset of online businesses offer "marketplace" and "crowd-funded" lending and investment, exemplified by Lending Club, in which borrowers or ventures are matched up with interested lenders and investors. (The same model is growing for charitable donation).

As discussed later, expanding online financial offerings will bring mixed impacts on consumers and will undoubtedly attract fresh regulatory attention.

Finally, a discussion of payments innovation is not complete without addressing digital currency. Whether labeled as digital-, crypto-, or virtual currency, the technology invented by Bitcoin is likely to have profound effects on the financial system, in general and for consumers specifically.

Created anonymously by people who mistrust government and sovereign currencies, Bitcoin's brief existence has featured mystique and high drama, including alleged scams, massive price volatility, and a high-profile trial involving murder for hire. While such developments tempt people to dismiss Bitcoin as exotic or criminal or both, regulators and central banks around the world are actively exploring the potential ben-

efits, as well as risks, of this very revolutionary technology.

Briefly, digital currency executes transactions on the internet rather than through the central payments and clearing system. Use of the internet platform creates transformative potential. Information moving on the internet—whether it is an email, a picture, or a financial transaction—is essentially free and instant and is globally accessible on a huge and growing scale. The internet is also an open platform, which means that in contrast to closed payment alternatives that require participating parties to join a system and accept a gatekeeper, digital currency enjoys advantages in massive, rapid, and decentralized innovation.

In addition, the creators of Bitcoin invented a powerful concept called the "blockchain," which is essentially an online distributed ledger of transactions. Owners of Bitcoin receive a "key" that is a unique and permanent, albeit confidential identifier. Every transaction flowing from that key is publically visible (and actively watched by numerous people) on the internet. This creates a public record of the flow of funds, which in turn can be a potent tool against fraud, against money laundering (despite some of the early incidents in that realm), and in almost totally preventing the ability to counterfeit funds.

The ingenious nature of the blockchain has sparked exploration of applications beyond movement of money. There are now several thousand companies in the "Bitcoin 2.0" space, working to apply this technology to dozens of use cases. There is potential to disrupt stock exchanges, making stock transfers instant and inexpensive, and inventing new stock ownership models, governance, and voting of shares—uses that will converge with the growth of crowd-sourced funding and overall network effects. Several countries are exploring creation of ledgers of companies, showing transparently who has ownership in what enterprises. Startups are working toward creating transparent and fluid markets for tickets, warranties, loyalty points, and government records like auto and real property titles. This trend could eventually disrupt industries like title searching and title insurance.

While Bitcoin itself may or may not survive as a dominant model, it seems clear that digital currency innovation will expand. *Cointelegraph* reports that venture capital investment in bitcoin-related entities rose 342 percent from 2013 to 2014, and that merchant acceptance reached 100,000 last year. Microsoft now accepts Bitcoin, as do growing legions of coffee shops. Investors increasingly include major mainstream parties.

As discussed below, virtual currency is likely to create enormous regulatory disruption and transitional challenges. One reason is that it transcends current regulatory structural models because it is three things simultaneously—a currency, an investment, and a platform for payment. The last of these three seems to hold the highest promise for transformative change. The new platform has the potential to disrupt the payment system itself, and/or to create a parallel system outside the banking system and thus outside the control of current central bank oversight and management. (*See the section below for a look at the many regulatory issues already arising.*)

Big Data

The second powerful driver of FinTech innovation is the growth of "big data" – information gleaned from external and nontraditional sources and used in marketing, designing, underwriting, pricing, and servicing financial (and other) products. While financial companies have long purchased information like direct-mail marketing lists, they are now finding transformative power in fast-growing digitized data that can be captured and manipulated electronically.

Sources of big data include social media, public records (property transactions, births, deaths, marriage, divorce, criminal and civil legal matters, and the like), GPS and satellite tracking, and cameras. A major growth area is the "Internet of Things" (IoT). This refers to the growing connectivity between the many small computers now embedded around consumers in items we own and with which we come in contact. Data exists and can be linked in everything from car keys and thermostats to televisions, baby monitors, home webcams, and the geolocation information in

phones and cars. People speak of "smart refrigerators" that can automatically place an online delivery order when the consumer is running low on milk—with a pre-arranged automatic payment. In February, AT&T announced that consumers can buy its new ultrafast fiber-optic Internet access for $70 a month, and for an additional $29 a month can opt out of having the company sell information on how they use it. In general, the default situation is that companies can obtain information about what people watch on television, video, and online; what they search on Google and what websites they frequent; what they do and "like" on social media; what they buy; where they live and travel; and much more.

When the IoT is combined with advancement in mobile, the impacts on consumers become ever more complex. Concerns are arising about the potential for hacking of digital devices not just to steal information, but to take control of them. Could criminals remotely seize control of a moving car and crash it, or assassinate a politician by hacking a pacemaker to induce a heart attack? While these risks extend beyond financial topics, they are illustrative of the regulatory challenges ahead. Consumers are already experiencing "ransomware" attacks in which hackers, rather than stealing money from an account, hijack a person's computer and demand a ransom, typically in Bitcoin, to release it. As payments capabilities are built into more and more interconnected devices, such risks are likely to rise.

Here again, impacts will be both positive and negative. As discussed below, beneficial opportunities include use of alternative data to enable more inclusive lending and other financial services for people who do not meet traditional credit standards. At the same time, concerns are rising about dangerous developments in privacy, data security, cyber-security, and "fairness."

Importantly, the growth of big data will be a two-way street. Just as businesses will know more about consumers, consumers will also know much more about businesses. Already websites are gathering, consolidating, and analyzing information about consumer choices—examples are BankRate.com and NerdWallet. As mobile services expand, this kind of information will be more and more comprehensive and easy to access, or will even present itself automatically as consumers make product choices. The kinds of product and provider ratings now available at sites like Yelp, Trip Advisor, and Amazon will come fully into the financial world, drawing on sources that range from straight product evaluation to burgeoning consumer reviews and government sources like the Consumer Financial Protection Bureau's (CFPB) databases on consumer complaints and Home Mortgage Disclosure Act (HMDA) patterns. Providers with low ratings, displayed adjacent to competitors with high ones, may feel a marked market impact.

Artificial Intelligence

Big data is notoriously challenging to use. It is drawn from disparate kinds of sources, making it difficult to normalize and integrate. It also tends to contain inaccuracies, partly because most of it is collected from databases where generalized accuracy is sufficient.

The solution to this is coming through developments in the third major tech trend – AI. Terms like "machine learning," "deep learning," and "neural networks" are entering the lexicon, referring to the fast-growing ability of machines to gather and analyze vast volumes of information in ways, and at speeds, hitherto unimaginable.

Computers today can take on a question or task; search all the digitized information in the world; analyze what might be responsive to the goal; suggest possibilities; learn from feedback; and endlessly improve results. In the medical realm, for instance, machines can diagnose cancer with accuracy rivaling and surpassing that of human pathologists, and can "collaborate" with humans to enhance the outcomes that either could reach alone. Importantly, machines have "noticed" things they were not even asked to find, such as characteristics of tissue outside a malignancy, bringing such observations to the attention of doctors who then have pursued new pathways of study and medical diagnosis.

Computers can conduct searches in seconds, hours, or days that would take humans hours, months, or even years to execute. They efficiently

synthesize images, data, and words, in any language, from across the globe, and then present analysis and conclusions in conversational language and useful graphics.

A critical factor here is that the machines are actually "learning." Their abilities have evolved beyond the stage where IBM's supercomputer Watson was able to win at chess and *Jeopardy!* Quiz shows are about finding facts and chess involves a finite set of logical calculations. Today's computers are moving beyond these capabilities into genuine thinking and even creativity. For instance, IBM created a "cyber-chef" that, while unable to taste food, is trying to develop recipes that optimize both appeal and nutrition at the same time, using ingredients and processes that humans would not think to combine. Success could conceivably cut modern risks relating to obesity.

In financial services, these kinds of innovations have tremendous impacts. Industry is using behavioral economics to create products and marketing that "nudge" consumers toward certain choices and behaviors based on sophisticated data analysis. Risk evaluation is being fine-tuned using more robust data and advanced algorithms. While the financial crisis created skepticism about statistical risk scoring, there is no doubt that new approaches are gaining momentum and widespread use.

Here again, the results will be mixed for consumers. More accurate risk standards can expand access for many people who now fail screening by legacy risk and data tools focused on broad categories rather than precision analysis of subsets. For instance, lack of traditional credit profiles, or adverse credit scores based on the limited data that gets reported to credit bureaus, can penalize some people who clearly have ability to repay a loan or deserve more advantageous pricing when looked at in a more individualized way. On the other hand, the reverse is also true—more precise evaluation will also find adverse factors among people who do well under current systems.

Furthermore, as discussed below, we are likely to see contentious debate on the intrinsic fairness of using factors that may be correlated with risk, or even truly predictive, but that nevertheless offend common conceptions about "fairness," and that trigger concerns about disparate impact in fair lending.

Beyond risk scoring, these new tools will also massively empower consumers with useful information that is convenient and customized. As an example, Goldman Sachs has purchased the company that makes Kensho, which can answer millions of complex investor questions in seconds. One can ask it, for example, how homebuilding stocks would be affected by a category 4 hurricane hitting the continental U.S, and receive an answer in seconds, in natural language text.

Again, this massive computing power will also tend to level the market's playing field by equipping consumers with increasingly helpful and accessible information about providers. New tools and resources will enable consumers to shop for and evaluate financial options based on aggregated data on performance and customer satisfaction. Aggregators will gather big data and apply AI to this task, producing ratings of individual providers and products and potentially screening out adverse product terms and pricing automatically, using a combination of personalized preference settings and expert guidance. This will tend to create a marketplace that rewards providers that earn and retain trust. Companies that today thrive on, say, fee income in areas their customers do not fully understand, may find new transparency placing them at a competitive disadvantage.

All this will raise novel questions about what entities will earn consumers' trust for playing roles like curation of their financial lives. Contenders may include traditional financial companies, large technology firms, startups, nonprofits, and potentially government agencies like the CFPB. Regulatory challenges will arise around potential disclosure and transparency regarding the profit models of such middlemen, as explored below.

Voice Technology

While it may blossom later than the trends noted above, natural voice recognition and response will almost certainly transform financial services. Today's voice systems, like Apple's Siri and Microsoft's Cortana, can already instantly respond

to fact-based questions and requests, like "Where is the nearest gas station?" or "Make a reservation at The Blue Duck for Saturday at six for four people." Amazon's Alexi, meanwhile, can execute spoken task requests like turning on lights or raising the thermostat in the consumer's home. Voice technology can also translate instantly from spoken to written text and vice versa, and can do simultaneous language translation, even mimicking the speaking voice and manner of participants in a conversation.

The new development is that voice technology is evolving into the ability to do true, interactive conversation in which the computer listens, "thinks," and responds much as a human would, rather than merely offering a one-way response based on finding facts.

Convergence of Tech Trends

As all four of these huge technology trends converge—convenient and ubiquitous mobile services, big data, AI, and voice technology—the marketplace will change profoundly.

For many consumers, voice-based services will be the final link in the chain that empowers them to take the reins of their financial lives. People who tend toward passive money management or who find financial choices confusing will suddenly be able to ask simple questions through their phones and get simple, spoken answers, rather than having to seek out information and read financial jargon and numbers. They will also be able to execute financial activities by voice, rather than having to go through steps they may find daunting or cumbersome.

Perhaps most importantly, they will be offered assistance—coaching—that will help them manage their own money habits and maintain focus on their goals. As noted above, for instance, the phone can warn them, through geolocation, if they are nearing a shop in which they tend to spend money that exceeds their budget—reminding them of how much they have recently spent there and where they stand in relation to monthly and annual savings goals or in saving toward a cherished objective like a new car, vacation, or college education.

Savings goals will be encouraged and reinforced through emotional behavioral science cues and motivators. Innovators are finding, for instance, that people pay more attention to savings when lottery-style rewards are introduced. Innovators are introducing social reinforcement in which people share a saving goal and encourage each other through texting or social media. Graphics are coming into use to intensify focus on a goal through pictures of it and visual ways of showing progress. BBVA Simple offers an account that enables people to insert photographs in their online statements. One customer created a mystery account and then revealed it to be saving toward an engagement ring – the couple later posted a picture of their marriage certificate. BBVA Simple's statement also features a number labeled as, "Safe to spend," rather than the account balance, encouraging customers to set aside adequate funds for fixed needs plus savings, and spend only the residual.

These kinds of changes will make it possible—amazing as it sometimes seems—to make money management fun and entertaining. Consumers will be able to customize their PFM tools to give their financial guides a personality and attitude. A parallel today is in MeetCarrot.com, which has a funny exercise app that calls itself, "Your judgmental fitness overlord." If financial tasks can become social and enjoyable instead of burdensome and boring, more people will perform them well. In the process, "financial literacy" efforts will leap into the phone, offering education just when consumers want it, and customized for their needs.

Again, though, the same technologies that drive every beneficial development will also be used to induce consumers to make choices that will be opposed by many in the advocacy world and in government. The same technology that warns someone not to overspend in a nearby store will also be used to encourage them spend as much as possible. The same technology that makes it easy to converse with a smart phone to manage an account will be used to foster choices that might have adverse consequences. The technology, itself, is morally neutral. Its impacts will depend on who uses it, why, and how. Regulators will have to navigate deftly through the complex task for

sorting "good" from "bad" and optimizing oversight of both.

Disruptive Impacts on Regulation

Returning to the kaleidoscope metaphor, all the trends above (and many other factors) will be shifting and combining in accelerating and constantly changing ways to impact the financial industry, products, practices, delivery channels, consumer preference and behavior, and regulatory responses. Remember, too, that technology convergence will bring some big, starling, seemingly sudden changes in areas that are quietly incubating now.

Innovation's mix of positive and negative effects will sometimes affect all parties and create tradeoffs in which certain parties (subsets of both providers and consumers) benefit while others suffer adverse consequences. These mixed impacts, combined with likely confusion over rapidly-evolving change, will inevitably bring political and policy pressures for and against various responses.

The players in this ecosystem (legislators, regulators, financial companies, attorneys and others) will confront two kinds of challenges in addressing these trends. First, they will often struggle to apply existing laws and regulations to novel developments. Second, they will gradually tackle the task of updating laws, regulations, and regulatory guidance to address new issues. Both of these situations will tend to generate high levels of uncertainty and inconsistency during a transition period. Furthermore, it seems likely that "transition" will actually be a permanent state—as soon as one new challenge becomes well-addressed, another, or many more, will arise.

Importantly, some of the innovations under discussion will *require* regulatory change, and some will *enable* worthwhile regulatory change that can address both emerging challenges and weaknesses of past regulatory approaches. The latter opportunity deserves proactive thought. There will be a natural tendency to address the former set of issues piecemeal and to layer new rules on top of old ones with only the minimum necessary level of harmonization. It seems possible, however, that profound shifts in technology can make it worthwhile to revisit fundamental aspects of old regulatory models.

Below are some of the most critical areas in which innovation will impact regulatory strategies. Again, these issues are highly interconnected and, again, it is not possible to foresee precisely how and when even the technology shifts will occur, not to mention how the regulatory process will respond to them. Still, many emerging challenges and opportunities are already clearly visible.

Overall Shift from Specific to General

Consumer financial protection regulation has tended to be framed around product categories. Numerous laws and regulations address consumer credit, and many address credit subcategories like mortgages, student loans, payday-type loans, open-end credit, and so on. Another group of laws addresses deposit accounts, while others cover investments, retirement funds, and other products. Many of these regulations require standardized disclosure (*see below for more on disclosure specifically*) and have detailed, product-based requirements. The "compliance" function has evolved with a heavy emphasize on perfecting technical adherence to these rules through technology and through technical subject matter expertise among legal and compliance personnel.

Several powerful forces are likely to shift this historic approach away from prescriptive rules-based regulation toward broad principles-based oversight.

First, the major technology trends heading toward consumer financial services will tend to transcend product categories and may be increasingly difficult to regulate through detailed prescriptive rules. As discussed below in more depth, the greatest challenges are likely to be in areas like privacy, data security, fairness in using big data, access impacts of new data and channels, and potentially the impact of digital currency. Generally, these shifts will touch every product category and will therefore be regulated through an overlay atop the product-specific rules. Not only will most of this regulation cover all of financial services, but much of it will cover more than finan-

cial services (although financial topics are likely to receive some specialized treatment).

Similarly, the emergence of mobile as a dominant channel seems likely to create new regulatory challenges that will cross-cut product types and transcend and stress some product-based rules. Mobile devices will increasingly be performing as financial products (handling the functions of a credit card, a prepaid card, a debit card, a deposit account, etc.); performing the functions of a payment tool, for both bill-paying and at point of sale; becoming a tool for shopping, evaluating, and signing up for a financial product choice; performing the function of applying for a financial services and of receiving disclosures and statements; providing a means of signing for payments or financial commitments and of lodging inquiries and complaints; and much more. This evolution will tend to create a misfit with existing rules and in some cases could cause difficulties with fitting new activities into traditional product categories.

A third factor is the speed of product change in today's environment. Formal rule-making is time-consuming, requiring months and often years of regulatory procedure. With products and channels evolving so rapidly, there is concern that the regulators will be unable to keep pace – that new regulations could be obsolete before they even become final. Situations needing legislation will move even more slowly.

It seems likely that all these factors will tend to push from rules-based to principles-based government. One can imagine a very suboptimal transition period in which both kinds of strategies coexist at a high level of intensity. Industry and regulators would be trying to adapt obsolete prescriptive rules to products and channels where they fit poorly, while industry would simultaneously face aggressive principles-based regulation and enforcement that has not evolved enough to produce principles that can be confidently applied.

The same trends seem likely to sharpen emphasis on broad-based regulatory topics, whether implemented through principles or rules, in addition to product-specific requirements. Key examples are UDAAP (addressing unfair, deceptive, and abusive acts and practices), privacy, data security, and inclusive access, as discussed below.

Finally, these broad trends will probably reinforce the growing trend toward bank regulators invoking "reputation risk" in supervision and enforcement. These agencies have the unique mission of protecting a safe and sound system and the security of Federal Deposit Insurance Corporation (FDIC)-insured consumer deposits, which makes them actively interested in risks *to* the companies they supervise, in ways not relevant to nonbank entities. Reputation risk can be a potent catch-all category that translates subjective concerns into supervisory action.

At least in theory, principles-based regulation has great advantages over prescriptive rules for addressing many situations, for all the reasons discussed above. Financial authorities in other countries (notably the United Kingdom), tend to emphasize it more than the U.S. has done. However, it only works well if regulators can wield subjective judgment with reasonable clarity and consistency. With FinTech changes coming so fast, and with our regulatory structure so fragmented (as discussed below), achieving clarity and consistency will be a challenge. A high priority of regulators should be to work toward shaping and articulating principles that can provide actionable guidance in the midst of rapid change.

Failure to achieve reasonable regulatory clarity and consistency will tend to drive providers out of consumer financial services, due to high and unmanageable regulatory risk. This is generally the opposite of government's goal.

Structure of Industry

Before turning to specific regulatory issues, it is worth stepping back to assess likely tech-driven changes ahead in industry structure, as these will directly and indirectly shape regulatory policies and strategies.

The coming changes will almost certainly have a complex impact on industry structures and on today's prevailing business models. By its nature, disruption brings realignment and creates winners and losers, both in the traditional industry being disrupted and among new entrants. Financial services will face extra challenges in this process because much (although not all) of the disruption

will be hitting banks, which are among the most highly regulated and supervised companies in the country, and which play critical economic roles beyond how well they serve consumers. These challenges are discussed further below under *Regulatory Structure,* but competitive changes to the industry are worth surveying before turning to specific regulatory topics.

First, it is likely that banks overall will lose market share to nonbanks, and possibly to companies that have a banking charter but provide mono-line services differing sharply from traditional bank offerings. This will create regulatory concern both about activities occurring outside the banking system, which tend to have lighter supervision (despite the broad scope of the CFPB), and about the health and safety and soundness of the banking system. Also, because banks are comparatively "easy" to regulate due to the robust existing infrastructure for doing so, regulators and advocates may seek to hold them to disproportionately high standards. This could put depository institutions at a competitive disadvantage in relation to less regulated rivals, in terms of both business opportunities and regulatory cost burdens. Such disadvantages would in turn exacerbate the trend toward banks losing market share, both due to competitive failure and potentially due to their opting to invest resources elsewhere.

It is noteworthy that this growing nonbank segment would likely include a wide array of company types, including startups that achieve scale; large technology firms like Apple, Google, Facebook, and Amazon; and other large players like telecom companies, which are often major financial services providers in other countries and have made entrees into the field in the U.S.

Second, proliferation of small FinTech startups will challenge regulators at all levels, simply because their size, newness, and numbers make them hard to find and monitor. These small players are typically licensed and regulated in their states, and many are seeking connections to banks that are raising regulatory challenges (more on this below). In addition, though, developers are creating money-related apps that can reach significant numbers of consumers with little or no regulatory clearance or scrutiny.

Another possible shift will be a further decline of smaller community banks and credit unions, which may be disadvantaged by consumers' increasing preference for high-tech channels and tools that smaller institutions are challenged to provide. Small institutions also face disproportionately high regulatory costs. Both of these may drive consolidation and maybe new, more efficient business models in this sector. While many institutions will undoubtedly pursue successful strategies, their numbers may fall further, creating serious impacts on many communities and significant political concern. Advocates for community banks are likely to intensify calls for two-tiered regulation that eases burdens on institutions that arguably have more community-focused business models and cultures and may not be widely engaged in practices that cause concern among regulators and consumer advocates.

A fourth structural impact, as noted above, is that some large banks may shift their business strategies away from consumer services when faced with new competition and rising regulatory requirements. Most large banks are working aggressively on tech innovation, especially in the mobile space, but many will find it hard to be fully competitive with companies entering the space with a clean slate and without costly legacy products and delivery channels. Most large banks in the U.S. also have highly siloed and aging technology in their primary activities, partly because so many have grown through merger and acquisition that has left them with patchworks of IT systems, and partly due to deferring major investment in integration. Many will struggle to compete fully with nimbler, simpler, higher tech players.

Nonbanks often critique banks for trying to take their current products and processes and digitize or mobilize them, without deeply rethinking them, and for working in siloes that view IT as an implementer rather than as an integral partner in innovation. Especially for the enormous millennial generation that will soon dominate the market, this approach may fail. One example is that while banks are busy (successfully) transferring their customers to online bill-paying, many millennials prefer to use other apps that essentially skip the

bank, other than as a store of funds. The mobile revolution will intensify this trend.

Inevitably, disruption of industry structure, and business models, especially when combined with novel kinds of consumer harm, will generate intense political pressures to protect one industry from another through legislation and regulatory policy. Policymakers will be wise to move toward developing principled arguments with which to navigate these waters.

"Fairness," Transparency, Simplicity and Disclosure (UDAAP and technical disclosure rules)

Challenges involving "fairness" include both fairness of product terms and practices, and fairness of access to the system. The latter is addressed below under the section titled "*Access.*"

Disclosure is the centerpiece of most consumer financial protection regulation. Providing disclosures to consumers is required under numerous laws, including the Truth in Lending Act (TILA), the Equal Credit Opportunity Act (ECOA), the Fair Housing Act (FHA), the Fair Credit Report Act (FCRA), the Truth in Savings Act, the Real Estate Settlement Procedures Act (RESPA), the Fair Debt Collection Practices Act (FDCPA), the Community Reinvestment Act (CRA), privacy law, securities law, a variety of specialized programs involving government-backed financial products, and much more.

Disclosure requirements are usually very detailed and are often combined with other highly prescriptive rules covering virtually all credit products, deposit products, investment products, and, at the state level, insurance products. The complex nature of these regulations has fueled the development of compliance systems, and in fact a full-fledged compliance profession, focused on tasks that are often (somewhat derisively) described as "box-checking."

It seems possible that the technology-driven revolution in information could lead to a deep rethinking of regulatory models built on mandatory disclosure. There is a widespread feeling that disclosure has been less than effective as a consumer protection strategy. While some benefit has undoubtedly flowed from requirements such as standardized calculations and terminology like Annual Percentage Rates (APR), there is extensive evidence that consumers do not find disclosures useful and tend not even to read them.

These concerns are already being addressed to some extent, including through the mandate in the Dodd Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank Act) that the CFPB develop consolidated disclosures for TILA and RESPA. Still, the benefits of the current disclosure laws may not outweigh their very high costs to providers—and ultimately to their customers—in terms of legal, compliance and processing complexity and exposure to penalties and costly corrective measures when errors are made.

This cost/benefit imbalance could reach a tipping point in an era in which people wanting to evaluate a financial product simply pull out their cell phones, as they might for evaluating a restaurant on Yelp or a product purchase on Amazon. As discussed earlier, the possibility exists that converging mobile, big data, and AI will equip consumers with better information than they receive now through disclosures. If so, it is possible that the disclosure framework will come under pressure for updating. Conceivably some disclosure requirements could be lifted entirely as no longer necessary. More likely, we might see more emphasis on how electronic information should and should not be presented. For instance, there is interest in widely mandating machine-readable product contract terms and offering them in publically-available databases, so that governments and third parties can compare, contrast, and analyze the details of product designs and pricing. If such a new mandate could be politically exchanged for reductions in old-style disclosure rules, consensus for action could arise. Consumers would potentially receive better information in more convenient forms, and industry could be freed of some of the current disclosure burden.

If we do see substantial growth in third-party product screening and mobile "coaching," there could also be new requirements relating to how they present product and pricing information, and in how the actual product providers must disclose information to them and through them

to consumers. Regulators may also move toward requiring transparency about business models for these mobile middlemen, coaches, and curators—do they make their money through fees to the customer, preferential referrals of providers, selling the consumers' data, or other means? Consumers could benefit from knowing. We also might see rules on financial advisory services migrating into these mobile services.

It also seems inevitable that a period of transition and comparative turmoil in how consumers receive information will ratchet up government emphasize on legal prohibitions regarding UDAAP. UDAP authority, with one "A" (omitting the "abusive" standard) has long existed for the Federal Trade Commission (FTC), the federal prudential bank regulators, and in most states. The Dodd-Frank Act gave the CFPB a mandate to address abusive practices as well. In the post-crisis era, all the federal financial regulators have aggressively enforced UDAP, and the CFPB has arguably made it the centerpiece of its regulatory strategy. This will continue for many reasons, including the shift toward more principles-based regulation predicted above. Again, these trends will create intense need for principles that are clear enough that industry can apply them with reasonable confidence, and regulators of all kinds will implement in consistent ways.

Another broad fairness topic is product "suitability"—whether providers should have a legal obligation to try to assure that product choices are appropriate for a given customer. This duty exists now in the investment realm but not in banking and was hotly contested during the Dodd-Frank Act's development. It could return.

The trends underway may also fuel existing interest in expanding two-tiered regulation, with lessened requirements for entities that are deemed to be highly "fair" to customers. This might include small community banks and credit unions, and/or providers of any size that offer only simple, inherently transparent products. There is a strong market move toward simplicity, especially in products targeted to millennials, many of whom exhibit low levels of "loyalty" to traditional banks but prize easy, simple products they access *a la carte*. Many startups are working on both credit and payments products that feature simple upfront pricing and are sold explicitly as an alternative to traditional services perceived as concealing confusing or tricky fees and terms. There will be discussion of exempting some such services from complex regulatory standards, including some disclosure.

The push for principles-based fairness and transparency will also fuel more regulators' efforts to post data publically, themselves, and to do so in ways that are easily accessible and useful in third-party analysis. In particular, the CFPB's complaint database is expanding and has been built with API (application programming interface) capabilities that foster easy uploading and analysis by others. The same is true of the HMDA database (see below). The CFPB has also launched online shopping tools for mortgages and student loans, aggregating market data and presenting it in ways they hope will draw consumers to their website for product comparison shopping. These trends will continue.

Finally, as noted earlier, tech trends like mobile and AI foster transparency and simplicity are likely to change the nature of consumer education, moving it from classrooms into the mobile phone, customized. Regulators are likely to try to foster and guide this process as part of a generalized drive toward "fairness" and information transparency.

Access (CRA, Fair Lending Laws, HMDA, Payday Lending Rules, Fair Credit Reporting Act)

As discussed earlier, the innovations underway are likely to have tremendous impacts on access to the financial system, many of them good, but some negative. There are two primary drivers of changes in access—mobile and big data.

The rise of mobile services will expand access for two reasons. One is that the mobile channel is an intrinsically low-cost delivery method, especially compared with the brick and mortar branch systems traditionally offered by retail banks and also by nonbanks like storefront payday lenders. Low-margin products and customer segments, like basic checking accounts and lower-income

consumers, will become more financially viable for providers when they can be reached through mobile services.

In addition, mobile services will increase access because, as noted earlier, lower-income and some minority consumers are disproportionately high users of such services, including for financial tasks. This is because many such consumers never adopted traditional online banking, due to the high costs of both personal computers and broadband internet access. Mobile services overcome both of those barriers. They also overcome many barriers arising from cultural, psychological, and knowledge sources. Many consumers who may hesitate to walk into a bank branch for fear of rejection or unfamiliarity with protocols are highly skillful in using their phones for a vast range of complex tasks, and enjoy doing so with some anonymity or distance.

Another positive factor in mobile is that the growing market is attracting many pro-consumer innovators into financial services, many of which explicitly describe their goals as improving access and fairness. Startups and sometimes large innovators are creating new approaches to small-dollar lending, checking accounts, and financial management apps, to name a few. The CFPB has created a program initiative called Project Catalyst, specifically to learn about and offer some regulatory leeway for promising innovation.

On the other hand, expanding mobile services will also constrict access for some consumers, especially in the short term. In particular, the trend will almost certainly bring widespread closure and/or repurposing of bank branches. This is already underway. SNL Financial reports that 2014 brought net branch closures of 1,462, with branch numbers declining to the levels of eight years ago. Transactions per teller are plummeting as more than half of banking has now moved online. Closures are disproportionately concentrated in low- and moderate-income and predominantly minority areas. Consumer advocates are very concerned that branch closures will harm lower-income and older customers who rely heavily on human, face to face personal service.

This concern has already begun to fuel debate on the future of the CRA. CRA performance standards currently evaluate the record of opening and closing branches and of providing alternative services. Almost inevitably, banks and regulators will find themselves under pressure to limit branch closures in low- and moderate-income neighborhoods. To the extent this succeeds, it will place banks at a market disadvantage at a time when nonbanks are vying for a rising share of the consumer financial market. There is also interest in having banks receive positive CRA credit for pro-consumer innovation that is not now rewarded under the rules.

Regulators are also concerned about adverse access shifts relating to payday lending moving increasingly online. Online short-term lending is growing rapidly in numerous forms, offered by offshore providers, through Indian tribal arrangements leveraging unique legal status, as an option by some of the major national storefront payday lenders, and again, by small providers including startups. Policymakers fear that easy access to some of these products will harm consumers who are unsophisticated or desperate. The CFPB released a proposed regulatory framework for payday-type lending in March, aimed in part at addressing these emerging issues.

If the CFPB's new approach to payday lending does not ultimately satisfy advocates, we could also see renewed focus on state usury laws and pricing controls.

The other major driver of access change—big data—was discussed extensively above. Again, growing uses of alternative data will inevitably make the financial system more inclusive and affordable for many people who lack traditional credit profiles, but will also screen out others. This shift will raise concerns under the fair lending laws—ECOA and FHA, and especially under regulatory doctrine that applies statistical "disparate impact" standards to lending. Disparate impact concerns involve businesses' use of policies and practices that unintentionally cause disproportionate harm to protected groups such as minorities and women. Findings of statistical disparate impact can trigger requirements that the business justify the practice, under standards that are generally subjective. The Supreme Court has

heard a case challenging applicability of disparate impact standards to housing and lending matters.

Regardless of the outcome of the pending litigation, these kinds of controversies are likely to intensify as big data evolves. Should people have their loans turned down because of what they "like" on Facebook, even if this is predictive? Such questions will be explored.

Inclusiveness goals in the era of big data may also drive changes in the FCRA. Regulators have concerns about whether traditional credit scoring and reporting are sufficiently predicative and inclusive. They also worry about inaccuracies in credit records—a topic the CFPB has highlighted. These issues, and the growing use of alternative data in risk rating and loan decisioning, could raise new thinking about the FCRA.

Finally, access issues are impacted by the HMDA, which requires that mortgage loan information be reported and made public to facilitate review of how mortgage lenders are serving minority and lower-income customers and areas. The CFPB is mandated by Dodd-Frank to expand this system to gather and report much more data. As noted above, the agency has also made HMDA data more readily accessible and useable through technology upgrades. The trends underway in innovation are likely to continue putting a spotlight on this topic.

It is worth noting that the CFPB also has a Dodd-Frank Act mandate to create a similar database for small business lending and loans to women- and minority-owned businesses. While this article focuses on consumer lending, most of the trends described herein will also impact small businesses and how financial companies serve them.

Privacy and Data Security

Almost all of the major technology trends have the potential to erode both financial privacy and data security (which overlap but are distinct). Both also are intertwined with anti-money laundering regulation, which will likely undergo many technology-driven regulatory changes but is beyond the scope of this article.

Also, both privacy and data security involve legal and regulatory frameworks that reach far beyond the financial industry but also involve finance-specific rules and enforcement. This multi-layered regulatory structure is likely to give financial companies a disproportionate share of change and challenge in the coming years.

Even as technology raises new consumer risks, it is also creating potential solutions that can bring consumers less exposure and more control. For instance, the advent of tokenization, as with Apple Pay, enables the processing of payments through a one-time authorization code that does not require merchants or others in the payment chain to access other personal information, including specifics about the credit card from which the transaction is drawn. Still, both fields pose huge risks.

Regarding data security, experts describe the challenge as a never-ending arms race between industry (and government) versus the criminals. It is commonly understood that data thieves are already "inside" all large institutions, and that they have developed new and complex ways to exploit data, including often showing patience in when they use it. An elicit network has emerged with complex sets of parties who break into accounts and who package and sell data, often in the "deep web" or "dark web." Strategies for intrusion vary, some targeting careless behavior by consumers using weak passwords and unprotected data in the cloud, while others infiltrate providers like banks and merchants. Many players in this activity are located offshore, and some are connected with foreign governments adverse to the United States.

Financial regulatory challenges surrounding data security are numerous, and all of them are intensified by growing use of mobile and big data, which can open up new avenues for data breaches and can increase the harm breaches do to consumers.

Discussion is arising over whether and how U.S. financial companies should be legally permitted to add offensive strategies to their defensive ones, with some large banks arguing for clearance to damage and destroy hackers that can be identified and targeted. Especially given the international nature of these crimes, this issue raises foreign policy complications and is contentious.

As data breaches grow in frequency, impact, and publicity, it is also likely that regulation and litigation will evolve over what parties are responsible for making consumers whole in what circumstances and how best to do so. Broadly speaking, consumers are protected from loss today for breaches that are not their fault. Their liability is also limited by the Electronic Funds Transfers Act (EFTA)/Regulation E and the TILA/Regulation Z if they promptly report a lost or stolen card, and consumers also have rights that trigger mandatory procedures when they dispute a payment. Nevertheless, laws are not fully clear or comprehensive in areas like when providers must disclose that potential breaches have occurred. There is also discussion of requiring remedies that are often provided voluntarily, such as services for identity theft detection and repair.

Another regulatory challenge involving data security is when and how to permit access to the banking system by third-parties, including vendors, partners, and parties to mutual referral arrangements. This issue raises other regulatory concerns, as discussed in the separate section below. On data security specifically, it is notable that Target's major security breach in 2013 was initiated through its air conditioning vendor. Bank regulators worry that consumer data can be breached by, or through, third parties that get access to it in the course of processing transactions, performing marketing roles, offering shared or co-branded products and other means.

Regulators and industry experts also express concern about the ability of the banking system, as a system, to withstand cyber-attacks. They note that the system is only as strong as its weakest link, which could mean that inadequate security by, say, a small bank or a third party vendor or partner in the payments chain, could enable infiltration of the system as a whole. While this is mostly beyond the scope of this article, it points toward further and likely legal and regulatory evolution relating to data and cyber-security.

Like data security, privacy involves the potential for consumers to have data about them used in harmful and unauthorized ways, and involves laws and regulations that are both unique to finance and broadly applicable to other industries. Furthermore, data insecurity is likely to lead to loss of privacy, as consumers' data may be sold or posted for public embarrassment, as has been the case with hacked celebrity photographs or the release of private emails among Sony executives in that company's data breach.

Nevertheless, there are important differences between the issues raised by privacy versus data security. Perhaps the most fundamental is that in data security, the interests of the customer and the industry are generally aligned—both are trying to protect personal data, and especially financial data. In the privacy realm, in contrast, the most contentious issues generally focus on areas where these interests are not aligned, in that the consumer may want (or is assumed to want) privacy protection from the same businesses that are otherwise serving them, or seeking to.

In February, the FTC issued a draft of a proposed Consumer Privacy Bill of Rights Act, aimed at updating and strengthening privacy protections affecting companies of all kinds. It arrives at a time when industry and advocates are grappling with the technology-driven innovations discussed above. Possibly more than any other emerging change, privacy raises profound dilemmas because potential consumer benefits and risks are so fully entangled with each other. Again, the emergence of big data and new data analytics are a force for greater financial inclusiveness and affordability and clearly fuel pro-consumer innovation, as providers look for new ways to tailor, price, and market products that are highly customized for each customer's needs and tastes. On the other hand, the public is likely to object to some of the ways in which such data are used.

There is evidence—albeit mixed—that a cultural shift is underway on privacy. Clearly millennials and younger consumers who have experienced only the digital age display comparatively high comfort with sharing information about themselves online. While some young people may be unaware that their social media postings and photos may be used by third parties, a great many fully understand it. While these young consumers often object to government intrusions into their private data (as reflected in, for instance, relatively high support for Edward Snowden and disapprov-

al of the NSA), few seem willing to forgo access to desirable technology and tech-based connections. Most consumers, of all ages, automatically hit the "agree" button on tech product disclosures that effectively sign away their privacy rights.

That reality may raise questions about the effectiveness and appropriateness of existing privacy laws. While medical providers adhere to the rules of the Health Insurance Portability and Accountability Act (HIPAA) and financial providers to those of Regulation P, data bundlers may easily discern that, say, a given individual probably has cancer or is in financial distress, based on the person's online searches that are generally fair game.

Accordingly, privacy law and regulation will be grappling with difficult issues. One is whether people should somehow be given meaningful control over their data and/or receive a fair value exchange for it. Sub-issues include whether such controls should be designed as an opt-in or an opt-out; whether they can be fine-tuned to avoid the situation where restricting one's data requires, in essence, withdrawing from digital life and commerce; whether compensation for data use can be implemented from a practical standpoint, including along a potential chain of subsequent users; whether compensation could be structured to provide a genuine discount for permitting data use rather than a surcharge for refusing to; and whether permissions, once given, can ever be withdrawn or terminated with respect to data already in motion.

Another emerging issue is whether to restrict collection of data to the narrowest scope necessary for a legitimate use. Sir Tim Berners-Lee, who is credited with inventing the Worldwide Web, recently told a Harvard payments conference that if his house key and lock must contain computers, he would like their relationship to be just between them, rather than residing in the cloud where it can be accessed, with or without legal authority, by others. Do data profilers need to know the time of day at which we go to work and come home, or how many people use our homes or cars? What limits should be set on satellite and drone surveillance of our movements, or use of infrared detection to "see" through walls at who is home and what they are doing? Public policy is moving toward trying to decide such questions, and use of financial data will be part of the debate.

In 1999, Scott McNealy of Sun Microsystems famously said, "You have zero privacy anyway. Get over it." Certainly personal privacy has eroded with, again, both good and bad effects for consumers. Whether it will be swept away in today's tide of innovation, or channeled through policy, will be worked out over the coming years.

Finally, experts suggest that the predicted growth in computing power, over approximately the next ten to twenty years, may drastically change some of these dynamics. It may be that consumers will not need to trade away their privacy for access to their digital goods, because they will have such vast power and control at their own fingertips, to get what they want, in the way they want it, forcing competitive providers to adapt.

Digital Currency

As noted above, digital currency is a mold-breaking innovation that spans multiple categories of financial activity, functioning (globally) as a currency, an investment, and a payments system. While the first two topics are complex, it seems likely that its greatest impacts will focus on the payments system. Again, these technologies could attract high volumes of financial transactions that do not clear through central clearinghouse functions, creating potential for destabilizing central banking activity and for forcing change upon it.

Despite this risk, central banks and regulators are generally (with some exceptions) exercising restraint in regulating virtual currencies and are not moving toward trying to block them (partly because much of this is almost certainly not stoppable in any practical sense). To the contrary, the Federal Reserve and other central banks are articulating a policy of observing and learning as the new system evolves, while ACH authorities are expressing interest in applying some of these new technologies to speed up their own functions, especially in the United States. Similarly, the Treasury Department's Financial Crimes Enforcement Network (FinCEN) is allowing room for evolv-

ing innovation, recognizing that this technology offers major potential advantages in combatting money laundering.

Digital currency companies like Ripple Labs are seeking to use this technology as a platform on which many kinds of transaction systems can operate with speed, efficiency, and transparency, including in both sovereign and alternative currencies. Other companies are creating digital currency exchanges; infrastructure to enable use of Bitcoin at point of sale, online and through merchants (at lower cost than use of credit cards); and ways of safeguarding consumers against Bitcoin's current, very active price volatility.

Among the numerous consumer financial regulatory issues in this realm are protection of Bitcoin retail investors from uninformed and unsuitable investments; taxability of Bitcoin transactions as capital gains and losses; management of money laundering and fraud risks; impacts on current rules affecting international remittances; and, again, how to capture the upside potential for consumers while blocking harm.

More broadly, the blockchain invented by Bitcoin may over time become a really revolutionary force toward a new and pervasive public transparency that would massively undercut privacy, in finance and everything else. People can envision a future blockchain that records how much power is used by a lamp, and when and where the lamp was made and bought, and by whom. Such a system would make today's big data challenges look elementary. Each potential Bitcoin 2.0 use case is uniquely and dauntingly complex, and those developing them are seeking to create markets that do not exist. Many predictions will never materialize. Still, big change seems inevitable.

The potential upside in consumer financial services is striking. If people could move their money instantly, at little or no cost, and in tiny amounts, globally, many intractable consumer financial problems would be abated. Beneficial new options could arise for financially-challenged consumers who now rely on a high-cost cash economy because they must closely manage timing of volatile income and expenses and cannot afford to wait for checks to clear. Instant crediting of payments would eliminate most of the problems now associated with account overdrafts and related fees. Driving down costs could also make it easier for industry to offer products like basic checking accounts.

These technologies are also likely to bring disruption to the international remittance market, by making payments cheaper and faster and removing complexities around currency fluctuation and cashing out the funds on the receiving end.

For the developing world, the impacts can be especially profound, providing a safe, formal, regulated system of payments and saving, for people who now have access only to cash or barter, and who conduct transactions in small amounts—equivalent to less than a U.S. dollar—that may not be cost effective to process in legacy financial systems.

Digital currency may be the fastest-moving and farthest-reaching innovation in the financial space. That speed, combined with its outside-the-box design and its decentralized and global nature, make it exceptionally complex as a regulatory challenge. Time will be needed to sort out the many new issues it will raise, and a transition period will inevitably be filled with uncertainty and problems as well as many new benefits.

Regulatory Structure, Strategies, and Processes

As noted at the outset, financial services are the first major industry to face disruption while being highly regulated, and regulated through a uniquely complex structural framework. We have five federal agencies that directly examine and supervise financial institutions (Comptroller of the Currency, FDIC, Federal Reserve Board, CFPB, and National Credit Union Administration (NCUA)). At least 20 federal agencies regulate some aspect of financial products, from mortgages and student loans to retirement funds, and/or have enforcement mandates that include financial services, as with the Department of Justice (DOJ) and the FTC. Much of this complexity is multiplied by fifty at the state level, plus insurance products are almost entirely regulated by the states. Large banks also face international regulators, while many kinds of business, such as telecoms offering financial products, must address requirements of

agencies like the Federal Communications Commission (FCC). The FCC will also be important as mobile services grow.

Not only are these agencies numerous, but they have complex sets of mandates. Some broadly regulate industries, as with banking, executing missions that include consumer protection but also have other goals like systemic financial safety and soundness. Some regulate products. Some address practices. Many have multiple regulatory tools that overlap those of other agencies – rule-writing authority, direct examination authority, enforcement powers, mandates for consumer education, goals of fostering certain financial products or assisting certain sets of borrowers, with regulatory oversight of compliance with their programs' rules and standards, and the like.

Any reasonably complex financial company is likely to be impacted by numerous federal and state (and sometimes even local) regulatory authorities unique to its financial offerings, over and above regulation that applies generally to corporations.

All or most of these regulatory bodies have at least fragmentary responsibility relating to the broad, overarching consumer protection themes discussed above, such as privacy, data security, UDAP, fair lending, and the like. As these and other regulatory standards shift and escalate under pressure from fast-changing technology, it seems inevitable that the complexity of this structure will exacerbate uncertainty and inconsistency in regulatory expectations, and will militate against modernization that might address problems efficiently and serve consumers well.

It is noteworthy that the single agency with the broadest scope and powers in this realm is the CFPB (full disclosure: I serve on the CFPB's Consumer Advisory Board, but do not speak in any way for the board or the agency). Created by the Dodd-Frank Act, it is relatively new and is uniquely empowered in several ways. First, it can supervise major market players and segments across the whole economy, rather than only through banks. Second, it has a very broad mandate and full spectrum tool kit, ranging from rule-writing and direct examination of large banks and some nonbanks to broad enforcement powers and even a charge to educate consumers. Third, Congress gave it responsibility for a large swath of the existing consumer protection rules. These factors have helped CFPB officials think holistically about many of the big trends explored in this article, and the agency has actively embraced an interest in innovation and technology. Nevertheless, the CFPB's powers and reach are still very limited. In many complex ways, it is just one player—albeit a powerful one—in the complex matrix of regulatory entities.

A whole cluster of regulatory structure questions revolve around what business should have what kind of access to the banking system. As discussed above, nonbank innovators need bank relationships in order to connect with the payments system. They all need bank accounts, and many are also seeking other kinds of bank relationships across a wide spectrum of arrangements, whether partnership, business development referrals, back end processing and servicing, and much more. Bank regulators are concerned about such entities creating risk to the banking system for all the reasons discussed.

These challenges are likely to spark some rethinking of how such system access issues affect innovation. In March, the House of Representatives held hearings on "Operation Choke Point," which the DOJ and FDIC have employed to limit banking system access for certain business types perceived to be high risk. FDIC Chairman Martin Gruenberg testified that the initiative's goal is to address risks that can enter into the financial system through types of businesses that are being used by criminal entities. On the reverse side of these same issues, innovators that are clearly pro-consumer could be blocked from system access by these kinds of policies.

A related issue involves state versus national licensing and chartering of FinTech innovators. Today, startups offering pro-consumer new products typically secure state licenses to do business (often in California). In order to grow beyond their home states, they must seek licenses in additional states. This is generally cumbersome and costly and can become a major barrier to achieving scale. Growing companies face a decision on whether to seek a federal bank charter, with its attendant regulatory complexities and costs, or to secure state licensing one at a time. One ques-

tion this raises is whether the federal government should offer charters that permit national scope for such companies, without the necessity to become banks. If so, it is not clear which federal agency would be the appropriate issuer of such charters, or what such a charter should cover and what rules should apply.

Alternatively, there is discussion of permitting more bank charters that are narrowly tailored for mono-line types of providers. More widespread use of such charters could produce chain reactions of questions about applicability of other banking regulations, including CRA.

Yet another aspect of this question is how regulators would view widened use of what is sometimes termed, "rent-a-charter" arrangements, in which banks form relationships with nonbanks in order specifically to give them indirect access to the advantages of a bank charter. More and more innovators are generating demand for these kinds of options.

Major issues also arise over whether to permit large nonbanks to engage in "banking" types of activities. The large technology firms—Google, Apple, Facebook, Amazon, major telecom companies—all offer some version of financial services, and several are likely to be aggressive players in mobile payments. Some of these companies may seek banking charters, and/or may increasingly offer services that customers perceive as the functional equivalent of a bank—absent the deposit insurance. Some such services may be highly popular and may, in fact, offer consumers superior and trustworthy financial choices. The regulatory system will have to grapple with whether to allow them into the formal banking structure or alternatively, how to protect consumers who may not understand the risks of being outside of it.

All of these bank-related issues will be challenging to address through the existing system of multiple bank regulators and with involvement by nonbank regulators that intersect with the topics.

Another regulatory structure question centers on how digital currency should be addressed. Again, it is designed to bypass the banking system and traditional processes for clearing payments. If virtual currency evolves to be a separate, parallel system, it could potentially open up activities that elude normal regulatory structures. If lower regulation attracts activity—which tends to happen—the existence of these markets will almost certainly spark unpredictable regulatory responses. Should virtual currency be regulated functionally, with different agencies separately addressing each aspect of what it does? If so, is there need for any coordination, some kind of pooled view into how it is evolving? State licensing laws and agencies often cannot even categorize the startups that apply for approval of these novel strategies. Responsible virtual currency companies are seeking regulation that will channel and legitimize this innovation. How to achieve that is complex.

A final question on regulatory structure and process is whether the pace and scope of technology change may argue for rethinking some traditional procedures. Could—and should—rule-making be speeded up? Should regulators consciously shift toward principles-based regulation that need less rule-making, and if so, how can they articulate principles that are clear enough to follow? Should they consider creating more safe zones for innovation and watching how it evolves? Could they commit to not penalizing well-intended innovation unless and until they issue clear guidance that requires providers to make changes? Should they try to move toward creating reliable regulatory "safe harbors" for very simple and transparent products, while applying principles-based oversight to more complex ones? Could financial businesses potentially earn a trusted status that would allow streamlining of oversight and regulatory burden? Could we learn to measure consumer outcomes rather than compliance inputs, as ways to assure good regulatory performance?

Could rule-making be entirely redesigned to mimic what innovators themselves do, using experimentation with trial, error and feedback before settling on solutions? Current rulemaking procedures are not only slow but also formal and stilted. Regulators and commenters essentially taking turns communicating, through hearings and especially through the back and forth of proposed rules and submission of comment letters. The agency lawyers then make decisions after reading these comments. They are smart people, but this process (which is surrounded by rules restricting *ex parte* conversation), is not conducive to, say, brainstorming innovative ideas. Might we

find better ways to foster interactive, collaborative dialogue, which seems to be more common in some other countries?

Regulatory restructuring is almost never politically achievable in the absence of crisis. Accordingly, the complex ecosystem of federal (and state) regulators will find themselves increasingly forced into closer collaboration and perhaps mutual deference on certain issues, or, failing that, will oversee rising levels of problems in the form of uncertainty, inconsistency, and both over- and under-regulation, likely including gaps between agencies in which public harm takes root — and which may later be difficult to weed out.

Conclusion

Political and regulatory systems naturally tilt toward detecting and addressing harm, rather than detecting and fostering—or at least not choking off—emerging positive change. After all, harm is often visible and concrete, while new possibilities tend to be invisible and diffuse. Normally, this tilt is probably a good thing, as government has limited ability in anticipating innovation and figuring out how to handle it.

In today's environment, though, the consumer financial regulatory system should strive consciously to become equally adept at both harm prevention and allowing "good" innovation to flourish. Eliminating harm, alone, would almost certainly stifle the potential for vastly beneficial change.

Doing this well requires shifting the regulatory conversation to focus more on these novel challenges, as the FinTech kaleidoscope moves with ever more complexity and speed.

NOTES

1. Jo Ann Barefoot is CEO of Jo Ann Barefoot Group, LLC, www.jsbarefoot.com.