HARVARD Kennedy School
MOSSAVAR-RAHMANI CENTER
for Business and Government

Digital Technology Risks for Finance: Dangers Embedded in Fintech and Regtech

Jo Ann Barefoot

June 2020

M-RCBG Associate Working Paper Series | No. 151

Mossavar-Rahmani Center for Business & Government
Weil Hall | Harvard Kennedy School | www.hks.harvard.edu/mrcbg

DIGITAL TECHNOLOGY RISKS FOR FINANCE:

DANGERS EMBEDDED IN FINTECH AND REGTECH

Fifth in a series of six papers on Regulation Innovation

Note: This is the fifth in a series of papers arguing that traditional regulation intended to promote consumer financial protection and inclusion has failed substantially and should be redesigned to leverage new digital technology that can make both finance and financial regulation better and less costly. For the previous papers in the series, see here.

Innovation has enormous potential to make finance more fair and inclusive, to make the financial system more competitive and healthy, and to make financial regulation more effective and efficient.

At the same time, it carries great downside risk. Technology is amoral, usable for both good purposes and bad. It also tends to create new problems as it solves old ones. In fintech, new benefits and dangers are often interwoven, making it challenging for policymakers to enable the former and prevent the latter. Similarly, in regtech, new techniques may either improve regulatory functioning or worsen it, depending on how new approaches are designed.

As discussed in Paper 6 in this series, regulators will struggle with both the content of new technologies and the exponential pace of change.

This Paper in the Regulation Innovation series explores technology-related risks arising from fintech and regtech, for both financial consumers and the financial system, and therefore for policymakers and regulators.

As explained in Paper 4, the challenges and opportunities involved in fintech and regtech innovation are distinct but highly overlapping, partly because both leverage the same shift to digital technology and therefore are built on the same foundation of new and better data. Accordingly, this paper will look at risks from both realms of innovation, together. Of course, in many areas, a key goal of regtech will be to block the risks arising from fintech.

The paper will look first at risks to consumers, and then perils and problems for other parties. For the most part, this paper will surface the risks without discussing remedies in any depth. Solutions will be explored in the final paper in the series, Paper 6.

Fintech's Risks for Consumers

The dangers posed by fintech to consumers can be broadly categorized around loss of privacy; compromised data security; rising risks of fraud and scams; unfair and discriminatory uses of data and data analytics; uses of data that are non-transparent to both consumers and regulators; harmful manipulation of consumer behavior; and risks that tech firms entering the financial or financial regulatory space will lack adequate knowledge, operational effectiveness, and stability.

A common ingredient in most of these risks is potential misuse and abuse of data. As discussed in earlier papers, digitized data is the lifeblood of innovation, enabling tremendous leaps toward expanded consumer financial health and inclusion. At the same time, it will inevitably bring problems. As noted in Paper 3, these issues all transcend finance, affecting nearly every sector. However, given the unique role of finance, and the uniquely pervasive regulatory system around it, financial issues will often be at the forefront as risks and problems are tackled through evolving public policy.

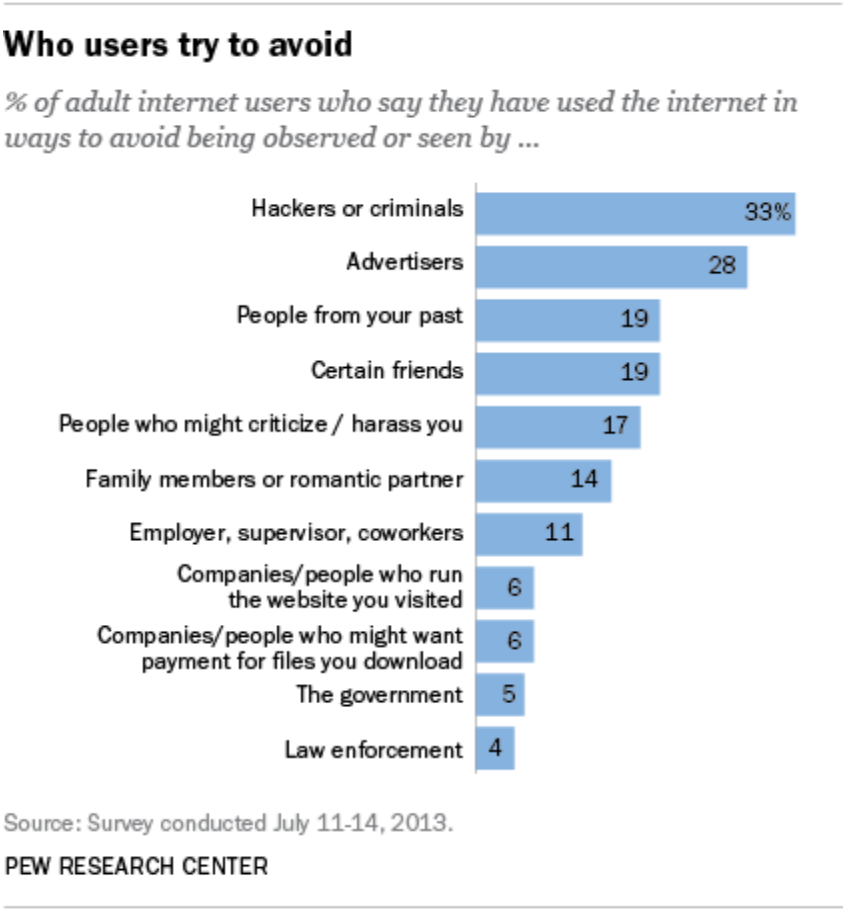
Privacy, cybersecurity, and fraud:

One major risk for consumers will be loss of privacy and data security. These two issues are intertwined and raise different kinds and degrees of concern depending on what consumer data is being accessed; how sensitive and identifiable it is; who is accessing it; whether that access is legal or illegal, and if legal, whether there should be more restrictions on use and whether consumers should be more empowered to see and reject certain kinds of uses.

A 2013 study by the Pew Research Center found that consumers are especially concerned about losing privacy to hackers and criminals.[1]

[1] http://www.pewresearch.org/fact-tank/2016/09/21/the-state-of-privacy-in-america/

Figure 14



Source: Pew Research Center

Privacy from government intrusion does not top consumers' list of concerns, but does engender contentious debate. Examples are the widely varied reaction to unauthorized data disclosure by figures like Edward Snowden or Julian Assange of Wikileaks, and the controversy over Apple's refusal to provide law enforcement agencies with a "back door" to the iPhone used in the 2015 terrorism incident in San Bernardino, California.[2]

[2] New York Times, May 21, 2016
https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=11&cad=rja&uact=8&ved=0ahUKEwiisdLWoofWAhVk6IMKHZ5tABUQFghdMAo&url=https%3A%2F%2Fwww.nytimes.com%2Finteractive%2F2016%2F03%2F03%2Ftechnology%2Fapple-iphone-fbi-fight-explained.html%3Fmcubz%3D1&usg=AFQjCNE6i28hbWUNg2KXTdgcuF4SC1rUrA

Concerns about data security are well-grounded. The 2015 data breach at the federal Office of Personnel Management compromised personally identifiable information like social security numbers on more than twenty million people.[3] The 2017 breach at Equifax exposed an estimated 143 million consumers to identity theft and fraud.[4] As discussed previously, banks are already at risk for data breaches due to aging and siloed IT systems in both industry and government. Identity theft is commonplace.[5] The Insurance Information Institute reports that $16 billion was stolen from 15.4 million consumers through identity theft in 2016, and the trend is rising.[6] The dark web runs thriving markets in stolen data which, depending on type and how long ago the breach occurred, can range from a social security number selling for a dollar and something like a PayPal account going for $80.[7] Cyber-insecurity is especially high in the developing world.[8]

The growth of these activities has spawned the grim phrase "Crime as a Service" – CaaS – playing off technology built around SaaS, or Software as a Service.[9] Hackers now optimize their activities by obtaining information and, rather than using it themselves, selling it to others – over and over.

As discussed in Paper 4, technology will help solve some of the same problems it is creating. Innovators are developing high-tech alternatives to relying on user passwords for security, since passwords are widely recognized as the weakest link in most security ecosystems.[10] Since people struggle to remember their passwords, they create guessable ones, or reuse them too much. Consumers can also be tricked into revealing them through phishing and spoof scenarios. Newer security options include using

[3] https://oversight.house.gov/wp-content/uploads/2016/09/The-OPM-Data-Breach-How-the-Government-Jeopardized-Our-National-Security-for-More-than-a-Generation.pdf
[4] https://www.consumer.ftc.gov/blog/2017/09/equifax-data-breach-what-do
[5] https://www.usa.gov/identity-theft
[6] http://www.iii.org/fact-statistic/identity-theft-and-cybercrime
[7] http://fortune.com/2016/08/03/social-security-dark-web/
[8] https://www.theguardian.com/global-development-professionals-network/2015/sep/24/mobile-money-apps-security-flaws-study-reveals
[9] https://www.entrepreneur.com/article/298727
[10] http://insights.wired.com/profiles/blogs/passwords-security-s-weakest-link#axzz4sxM7926w

biometrics like thumbprints, retina scans, ear contours, and even distinctiveness of gait or computer keystrokes.

Similarly, as discussed in Paper 3, a new generation of promising solutions is arising in the form of Privacy Enhancing Technologies (PETs) such as homomorphic encryption, zero knowledge proof, and differential privacy techniques. These, combined with widespread conversion to digital identity systems rather than insecure analog ones (since, again, the analog information is widely compromised and for sale), could create data environments in which consumer information is much more secure and is much more subject to the consumer's own control.

As Paper 6 will discuss, there is also a robust industry discussion on the desirability of moving away from the analog-era approach of collecting data and storing it all in a central place, since these huge databases can become "honey pots" that attract hackers and cybercrime. A new concept is to leave data decentralized and analyze it where it is. Giant Oak CEO Gary Shiffman has termed this concept, "the traveling algorithm."[11]

Nevertheless, experts predict a permanent "arms race" between security professionals and criminals, with no full technology solution likely. The Internet of Things, or IoT, will increase vulnerability by connecting more and more sensitive data through more and more devices, each of which can be attacked.[12] The IoT connects up the many smart devices that increasingly gather data about consumer activities and makes it available for various uses. IoT devices include smartphones, automobiles, other geolocation trackers, cameras, watches, wearable fitness devices, electronic keys, smart thermostats, and smart appliances like refrigerators that automatically order more milk or washing machines that reorder detergent. Headlines like, "Hacked by Your Fridge" have become common.[13]

Consumer data rights:

[11] https://www.jsbarefoot.com/s/Shiffman-Podcast.pdf

[12] http://www.cnn.com/2014/01/17/tech/gaming-gadgets/attack-appliances-fridge/index.html

[13] http://theconversation.com/hacked-by-your-fridge-the-internet-of-things-could-spark-a-new-wave-of-cyber-attacks-66493

Risks to consumers may also arise over whether and how they can give permission to third parties to access their bank account data in order to perform tasks for them, such as letting financial apps help them save money. As discussed in Paper 3, numerous fintech innovators rely on this permissioned access. However, some banks have argued that these uses may be insecure and that, in the event of breaches or loss, customers may blame the bank for allowing the fintech to use the data.[14] This issue is raising questions about who actually owns a consumer's bank account information – the customer or the bank? Europe has taken steps to provide customers with rights to their data and with portability of bank accounts.[15] Fintechs generally contend that a consumer's bank account information belongs to him or her, not to the bank, and that financial customers should be able to move their records in much the same way that medical patients can move an x-ray from one doctor to the next.[16]

Consumer harm may arise from inadequate control of these permissioned-access models. It can also arise if either banks or regulators shut these innovations down, throttling promising financial technologies. The issue may require regulatory clarification regarding liability for harm in the case of breaches or errors. At this writing, the issue is under review by the CFPB.[17]

A key concern in this space is how to establish liability in the event that consumers' data is compromised, in situations where it may be unclear which entity failed to protect it. Again, banks worry that they will be blamed, legally and in terms of reputation damage, even if it is the fintech that made the error. Sometimes it is not possible to fully trace the source of an error. Even where it is, banks fear that their size and resources will make them litigation targets, as opposed to small, impecunious fintechs.

---

[14] https://www.jpmorganchase.com/corporate/investor-relations/document/ar2015-ceolettershareholders.pdf
[15] https://www.evry.com/en/news/articles/psd2-the-directive-that-will-change-banking-as-we-know-it/
[16] https://www.americanbanker.com/news/fintech-companies-form-lobbying-group-focused-on-data-sharing
[17] http://files.consumerfinance.gov/f/documents/112016_cfpb_Request_for_Information_Regarding_Consumer_Access_to_Financial_Records.pdf

In this area, too, there are nascent ideas for technology-based solutions. These include the potential to use blockchains or other technology to make data movement traceable electronically, to pinpoint the specific source of breaches and leaks when they occur.

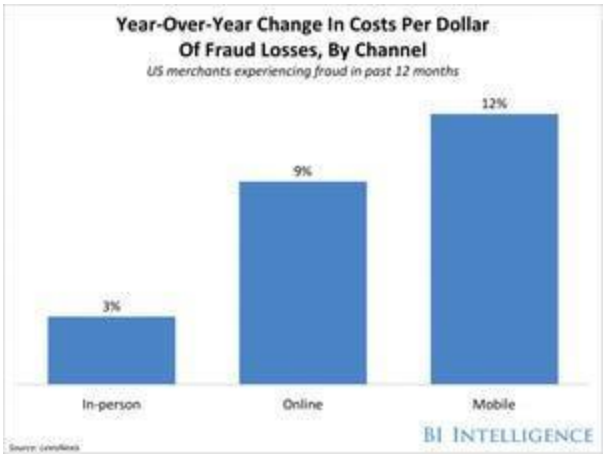
Fraud and scams:

Along with cyber-insecurity, consumers will face the related risk of rising fraud and scams.

Scams are especially harmful to vulnerable groups of consumers. The National Council on Aging reports increased targeting of senior customers,[18] and similar predatory patterns aim to exploit people with disabilities.[19] Paper 3 discussed the rise of scams against people for whom English is a second language.

Broadly speaking, online and mobile channels are also subject to far higher rates of fraud than are branch-based services. It is easier to assume fake identities online than in person.[20] It is also easier to build the "synthetic identities" discussed in Paper 4. Online payments channels are also extensively impacted by "friendly fraud," in which real consumers make credit card purchases, keep the merchandise they buy, and then exploit the consumer protection laws to make claims of unauthorized charges,[21] in order to keep both the goods and the money.

Figure 15



[18] https://www.ncoa.org/economic-security/money-management/scams-security/top-10-scams-targeting-seniors/
[19] http://disabilityjustice.org/financial-fraud/
[20] https://www.businessinsider.com/online-lending-is-making-fraud-easier-2016-10
[21] https://www.verifi.com/kb/what-is-friendly-fraud/

Source: Business Insider, October 31, 2016

Fraud losses do indirect harm to consumers both by raising costs and by causing some legitimate customers to be screened out of financial access – especially those with identity information that is harder to verify, such as immigrants and young people.

These problems are also rising in the developing world where millions of people have newly entered the financial system with phone-only financial services and have little or no previous financial experience to help them navigate it.[22]

Fairness and "computational ethics:"

Another data-related risk for consumers centers on questions of fairness in how new types of data are used. As discussed in Paper 3, the availability of nontraditional data can bring tremendous benefits, enabling financial companies to authenticate identity and safely underwrite loans to people with complex credit profiles. However, concern is rising that these same processes could be misused or abused as financial companies leverage new data and AI in algorithmic analysis to guide business decisions like targeted marketing, pricing, and whether and how people qualify to open accounts or receive loans.[23]

Here again, those worries are exacerbated by the growth of IoT. Consumers' activity can be tracked today to analyze online media activities, entertainment choices, shopping habits, and location. In-store cameras can interpret reactions to merchandise. Voice analysis can assess emotion, including through interaction with robots.[24] In addition, government records are being rapidly digitized, enabling varied data to be combined with readily accessible information on factors such as birth, death, marriage, divorce, criminal and civil legal matters, tax judgments, property and vehicle titles, real estate sales, property tax assessments, and much more.

In short, a massive expansion is underway regarding compiling and use of data from many sources. This includes information that has always been publicly retrievable but was costly to acquire and

---

[22] http://www.cgap.org/sites/default/files/Brief-Fraud-in-Mobile-Financial-Services-April-2017.pdf

[23] A Government Accountability Office report on these issues is expected in the fall of 2017

[24] https://www.theguardian.com/technology/2017/may/05/human-robot-interactions-take-step-forward-with-emotional-chatting-machine-chatbot

consolidate; data that is private, sensitive, and theoretically restricted to certain use, like financial and health information; and data that is less private and may even be anonymized but will increasingly be used to benefit or disadvantage people, as discussed below. As these kinds of data become increasingly consolidated and digitally accessible, the public's concern about data breaches, identity theft, and legal or illicit use by government and private entities can be expected to rise.

Concerns are also growing about what is done with all this data, especially through artificial intelligence. AI often produces "black box" data models and decisions that cannot be readily evaluated by humans, and which may, intentionally or not, produce discriminatory or otherwise inappropriate outcomes. Cathy O'Neil, in her book *Weapons of Math Destruction*, describes problems arising from use of AI in realms like criminal justice and evaluating the performance of public school teachers.[25]

As explained in Paper 3, the cutting edge of innovation lies in the combination of having new data to analyze, and analyzing it in new ways – i.e., at the juncture of Big Data and AI. Issues are arising in both realms, regarding both the data being analyzed and the methods used to analyze it. Issues can be classified broadly around whether the data being used is accurate;[26] whether the data set is sufficiently large to permit analysis for the purpose at hand; whether the model is using data elements that may act as proxies for prohibited factors such as race or gender; whether the model's "training data" sets may be importing inappropriate biases due to "learning" from human decision-making that was already biased; how to evaluate whether the model is in fact highly predictive of risk (especially for use in long-term scenarios like mortgage lending, or any lending that has not been tested over a full credit cycle); and whether the model can be audited by regulators and other risk reviewers to determine, among other things, whether it is both predictive and fair under the law.

[25] https://weaponsofmathdestructionbook.com/

[26] Financial companies are expected to assure high accuracy of most sensitive, personally-identifiable customer data. In contrast, many sources of big data contain high levels of inaccuracy, sometimes because the reason for their original collection did not require high accuracy. Reusing such data for other purposes can raise issues.

Jeffery Rayport has argued in *MIT Review* in favor of adopting data principles to guide the answers to such questions, focusing specifically on "clarity of practices," "simplicity of settings," "privacy by design," and "exchange of value."[27]

Auditability can be a particular problem for AI that involves highly confidential intellectual property. Even more basically, data scientists often warn that there is, broadly, an inverse relationship between explainability and predictiveness in AI risk and forecasting models.[28] As the machines take their learning to advanced stages, humans sometimes simply cannot tell why certain models make more accurate predictions than others, and whether those reasons comport with our standards of legal and ethical practice.

Technology and financial industry organizations are moving to address this range of challenges, focusing on concepts such as "explainable AI,"[29] "computational integrity," and "computational ethics." Many parties are discussing development of standards or best practice.[30] Privacy advocates have urged establishing a code of ethics or code of conduct for data professionals, arguing that, like doctors or lawyers, they play a crucial role in society and should subscribe to principles requiring them to "do no harm."

Discriminatory "disparate impact:"

As discussed in Paper 2, U.S. laws generate a particularly contentious subset of the data fairness issue due to legal prohibition of a form of discrimination known as "disparate impact" in lending. Unlike "overt" or "disparate treatment" discrimination, disparate impact arises when a lender uses a practice, product design feature, or underwriting standard that treats all individual customers consistently, but produces a statistical outcome that is disproportionately adverse for members of "protected classes" based

[27] https://www.technologyreview.com/s/424104/what-big-data-needs-a-code-of-ethical-practices/
[28] https://www.content-loop.com/artificial-intelligence-can-go-wrong-but-how-will-we-know/
[29] https://www.accenture.com/us-en/blogs/blogs-why-explainable-ai-must-central-responsible-ai
[30] An example is Immuta, https://techcrunch.com/2017/04/25/immuta-adds-accountability-and-control-for-project-based-data-science/

on factors like race, ethnicity, national origin, religion, sex, sexual orientation, or receipt of public assistance.

A simple example occurs with lenders that set a minimum loan size, below which they will not extend credit. A bank might say that it will only make mortgage loans above $100,000, because smaller loans cost as much for them to underwrite as larger ones, but produce less profit. This policy would affect every individual applicant equally, but might disproportionately impact minorities if, in the bank's market, these customers are disproportionately likely to buy lower-priced homes needing smaller mortgages.

Practices that produce such impacts can be challenged based on statistical analysis. If statistical disparate impact is shown, the lender must then demonstrate a valid business justification and show that another, less discriminatory approach cannot meet the business need. Merely demonstrating that a factor accurately predicts risk is not legally sufficient. (This legal standard contrasts with those impacting the insurance industry's use of actuarial risk mathematics, and is also not the norm outside the U.S.).

The rules of the road for disparate impact enforcement in credit are not fully clear. The disparate impact or "effects test" concept originated in employment law and also applies to housing discrimination, but regulators have provided only limited guidance about how it applies to credit which, unlike a job, house purchase, or apartment rental, does not produce zero-sum competition among applicants. Accordingly, there is uncertainty about what kinds of data are legal to use.

Analogies arise outside the lending realm. In functions like fraud detection, where disparate impact doctrine does not apply, measurable risk indicators have been found in areas like consumers' social media habits, time of day or night that people are online, and whether a customer fills out an application form in block letters (presumably because fraudsters may use that method to disguise handwriting). In insurance, expanded IoT data may enable companies to evaluate and price coverage based on the consumer's wearable fitness tracker, smart scale, or even factors like eating habits. Google's data could enable insights such as that a person has cancer or is engaged in an extramarital affair that could lead to financial instability.

The lending arena raises all of these kinds of fairness challenges, and essentially supercharges them due to the additional, specific laws barring disparate impact. Confusion abounds, including whether use of a given underwriting factor should be logically linked to risk "causation," or whether lenders should be able to rely on high "correlation" with loan outcomes, without knowing why they occur. Raj Date, founder and CEO of Fenway Summer LLC venture capital fund and former acting director of the CFPB, has noted that a highly predictive factor for creditworthiness is whether people pay for gas at the pump or go into the station.[31] The theory is that, on average, people who pay inside are more likely to be smokers, and smokers are more likely to be poor credit risks. As more and more data become available and analyzable with AI, it will be increasingly difficult to draw lines between acceptable and unacceptable risk factors.

The dilemma is especially challenging because, as discussed in Paper 3, use of new data types are showing great promise to make lending *more inclusive*, not less so. An example is the controversy cited earlier regarding use of alternative data in underwriting. Early research suggests that capture of alternative data, such as bank records showing the customer's cash flow, can enable lending to many people who are currently screened out by traditional credit scoring, and that this can be done without loss of loan quality.[32]

Again, the regulatory standards for deciding what data can be used and how to demonstrate a business justification if disparate impact occurs are unclear.[33] The result is that, today, most lenders do not employ alternative data, even if they are confident that it could enable them to reach more people with sound loans and to adjust loan risk-pricing in favor of large numbers of consumers who appear riskier than they actually are, when evaluated only with traditional data like credit scores. Nevertheless, increasing numbers of lenders, especially startups, are starting to do so.

---

[31] http://www.jsbarefoot.com/podcasts?month=April-2015

[32] https://finreglab.org/reports/cash-flow-data-underwriting-credit-empirical-research-findings

[33] Virtually all traditional lending standards already produce disparate impacts, but they are "safe" to use because they are established as standard practices that are acceptable to regulators.

Overall, then, disparate impact and new data raise two risks for consumers. One is that lenders will use unfair data standards. The other is that regulatory uncertainty will prevent lenders from expanding access to sound, affordable loans for more people.

U.S. regulators are taking steps to increase clarity. The CFPB has evaluated this issue with both risks in mind,[34] and has also issued a No Action Letter, or NAL, on the topic.[35] In addition, in December 2019, five federal financial regulatory agencies issued a joint statement encouraging exploration of using alternative data in loan underwriting.[36]

Behavioral manipulation:

Another set of concerns about fintech innovation focus on the risk of behavioral manipulation. The same technologies that can help customers better manage their finances and habits have a dark side, potentially enabling providers to induce overspending, over-borrowing, and use of inferior or more expensive products. Again, providers will have massive data on people, will know a great deal about their lives and personality types, and will have tools such as human-like voice assistants and engaging chatbots that offer interactive advice. Harvard University's Cass Sunstein has identified the ethics of "nudging" as a critical issue, one that will challenge business and government alike.[37] The same techniques that can help people save rather than spend, can also make them spend rather than save.

These fears also raise a concern that, manipulative or not, the sheer convenience of fintech will make spending "too easy." The financial industry speaks of the "uberization of payments," meaning the disappearance of the payments process into the experience being paid for, as when one exits an Uber car without any money or paperwork changing hands.[38] Disconnecting the purchase process from the

---

[34] https://www.consumerfinance.gov/policy-compliance/notice-opportunities-comment/archive-closed/request-information-regarding-use-alternative-data-and-modeling-techniques-credit-process/

[35] https://www.consumerfinance.gov/about-us/newsroom/cfpb-announces-first-no-action-letter-upstart-network/

[36] https://www.occ.treas.gov/news-issuances/news-releases/2019/nr-ia-2019-142a.pdf

[37] Cass Sunstein, "Do People Like Nudges?" https://web.archive.org/web/20170705164340/https://www.hks.harvard.edu/content/download/76976/1728463/version/1/file/RPP-2015_14_Sunstein.pdf

[38] https://www.paymentssource.com/opinion/the-uberization-of-payments-pressures-security-and-e-channel-strategies

payments process could exacerbate the widespread human tendency to spend more than one should. Similar questions have arisen about Amazon and especially Amazon Prime, whose members spend more than double the amounts of non-Prime customers.[39] The flipside of hyper-convenient, friction-free payment could be over-consumption and under-saving, echoing the patterns that emerged as credit cards displaced hard cash, and net savings rates declined.[40]

Real-time and peer-to-peer payments:

Related concerns also arise around making the payment system faster, and even instant. Many consumer advocates believe that people often benefit from having some "friction" in the payment process, to allow a cooling off period after some spending activities – examples are being able to stop payment on a paper check or cancel an online payment before it clears. The same delays can help protect people from online scams and fraud.

The U.S. system for clearing payments is slower than those in much of the rest of the world. In 2019 the Federal Reserve announced its plans for developing a real-time payments system,[41] a project that has sparked some debate relating to optimizing the roles of the public and private sectors.[42] One way or the other, more rapid settlement will clearly develop.

There are concerns about potential risks relating to popular peer-to-peer payments systems that partly or fully by-pass central clearing through banks.[43] When such alternatives are less regulated than banks are, critics fear the potential not only for data insecurity and consumer protection violations, but also for the possibility that the fintechs involved may experience liquidity problems, as has happened in cases involving, for instance, prepaid cards.[44]

---

[39] http://www.businessinsider.com/amazon-prime-members-may-spend-more-than-double-what-non-members-do-2015-1

[40] https://www.livescience.com/2849-study-credit-cards-spending.html

[41] https://www.federalreserve.gov/newsevents/pressreleases/other20190805a.htm

[42] https://www.wsj.com/articles/banks-confront-fed-on-faster-financial-payments-11564911000

[43] An example is https://venmo.com/

[44] https://www.nytimes.com/2016/05/14/business/dealbook/rushcard-to-settle-prepaid-card-suit-for-19-million.html

As discussed in Papers 2 and 3, faster payments have the potential to solve enormous problems for millions of consumers who have cashflow difficulties. Such customers pay large volumes of bank overdraft fees. Millions also pay premiums for check-cashing services, so that they can convert just-received funds immediately into cash with which to pay bills in time to meet the due dates. Still, fast payments will produce mixed results for many consumers.

Opaque business and profit models:

Another related risk surrounds the likely expansion of business models that are not transparent regarding how they make money. This issue already exists but is likely to expand as more types of players interface with consumers, and especially with services and apps that purport to provide trustworthy advice or help in making financial choices.

These advisory entities have only a few ways to generate revenue. They can charge a fee (thus far, most online efforts at this model have not worked well). They can charge a commission, such as on investment trades or percent of investment portfolio. They can be embedded in a revenue-generating product, such as loans or investment services or perhaps retail goods – for instance, Amazon could use sales of goods to subsidize advice services. Companies can also be paid by third parties to refer the customer to them. Last but not least, such firms can profit by selling the consumer's data.

All these models exist today and can be legitimate, but most also have the potential to be misleading or potentially abusive.

Erosion of financial literacy:

As noted in the previous section, there is also concern that easy and automated financial management will undermine the long-standing drive for higher financial literacy. If people lack even a basic understanding of finance, they will be more vulnerable both to inadvertent technology failures and to predatory practices, unless their technology is actually failsafe in protecting them. An analogy is GPS navigation; if it makes an error, and one has no map and no bearings, the technology benefits can quickly become liabilities.

Technology advocates counter that consumers rely on well-regulated technology to protect them from many kinds of risks they don't understand, from the safety and efficacy of medicines to the drinking water flowing from their taps. Josh Reich, CEO of Simple, has compared this consumer education challenge to the evolution of automobiles from standard transmissions to automatic ones that made it easy for almost anyone to drive[45] (not to mention the potential for autonomous vehicles). Much debate is likely to center on these issues.

Proliferation of providers:

Policymakers will also have to fashion ways to regulate very small innovators, which will be able to reach consumers on a scale never before imagined. Small startups are likely to be disproportionate sources of both beneficial new ideas and rising harm such as incompetent advice and operations, fraud, and high rates of business failure that can leave customers stranded. While bank regulation has failings, it has the virtue of comparatively easy oversight over a finite set of companies. Today, the proliferation of fintech startups means that customers are increasingly getting financial services from companies that are not banks and may not be licensed by a state, either. As noted in Section 2, state-licensed providers number in the hundreds of thousands in the United States, which means they are too numerous to be closely monitored through traditional regulatory means. Paper 4 discussed the challenges regulators face in "policing the perimeter" of the sprawling financial system.

This situation can raise many kinds of risk. For instance, companies in the payments realm take in customers' funds and then pay them out to the intended recipient. If such a company fails or has a technology disruption, the consumer's funds could be unavailable when needed, or even lost. Such a failure occurred with the RushCard prepaid debit card, with thousands of customers unable to access their funds for days, causing cascading financial harm.[46]

---

[45] http://www.jsbarefoot.com/podcasts/2015/5/4/episode-2-the-cheerful-disruptors-with-josh-reich-and-shamir-karkal-from-simplecom

[46] The CFPB fined Rush Card and its processer Mastercard https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=3&cad=rja&uact=8&ved=0ahUKEwi17Lr4q4fWAhXr54MKHWa8BN4QFggyMAI&url=https%3A%2F%2Fwww.nytimes.com%2F2017%2F02%2F01%2Fbusiness%2Frushcard-cfpb.html%3Fmcubz%3D1&usg=AFQjCNHu5t407R8LNgF1Oz4bGz5YS7AwFQ

Concerns also arise over small startups and consumer apps having insufficient infrastructure to assure cybersecurity and regulatory compliance (although, counterintuitively, many fintech startups are actually superior in those functions because they have started with a clean slate and new technology including secure cloud computing, avoiding the problems many banks experience with legacy IT systems).

Undermining of usury laws:

Many consumer advocates oppose aspects of fintech innovation that enable companies to avoid coverage by state-based usury laws that cap interest rates on consumer loans. Extensive litigation has occurred over the circumstances in which fintechs can rely on their partner banks, in situations where the bank technically extends the loan but may not retain it.[47] Many consumer groups also opposed the proposal of the Comptroller of the Currency to create a special national bank charter for fintechs, a move that also sparked litigation by the State of New York and the Conference of State Bank Supervisors.[48]

Other Risks from Fintech Innovation

The previous section focused on risks to consumers arising directly from their use of and exposure to fintech. While the Regulation Innovation series centers on consumer financial regulation, it is nevertheless important to consider additional risks that will arise from fintech's potential to disrupt the system overall, which will have impacts on customer wellbeing as well as other regulatory objectives. The following section looks at these hazards, while the subsequent one explores risks likely to arise directly from adoption of digitally-native regtech.

Systemic risk:

Fintech innovation could undermine financial system stability in multiple ways.

One is the possibility that banks will fail to innovate sufficiently and will therefore lose market share. This does not appear to be happening yet, as reflected in the World Economic Forum study cited

[47] https://www.cato.org/blog/invalid-when-made-district-courts-madden-v-midland-decision
[48] https://www.nacha.org/news/federal-judge-dismisses-csbs-second-lawsuit-against-occs-fintech-charter

earlier. It found that innovation is clearly altering financial products and practices but not, thus far, the industry's structural makeup. Few fintech startups have reached sufficient scale to rival banks. The study does, however, point to the potential for Big Tech firms like Amazon, Apple, Facebook and Google to become major financial players if they so choose.[49] *Breaking Banks* author Brett King makes a similar point, predicting that by 2025, the world's largest bank will not be a bank, but rather a technology giant -- China's Ant Financial. He notes that in 2016, Ant's Alipay system processed $17 billion in mobile payments in a single day.[50]

If growth in the financial industry moves increasingly outside the traditionally regulated banking sector, many challenges could arise in the U.S. and globally, with impacts on monetary policy, the functioning of central payments systems, and the ability of regulators to monitor and manage changing systemic risk as it emerges outside their direct line of sight (as happened with the subprime mortgage lending that sparked the financial crisis). Within the banking industry, these kinds of shifts could potentially create liquidity or reputation crises as well as bank failures.

Policymakers in a number of countries have taken steps to require or encourage "open banking" [51] -- electronic sharing of bank account information, with the customer's permission, usually through an API. The UK required banks to permit such sharing through its Second Payment Services Directive, known as PSD2.[52] Open banking is used by customers who want to allow fintech companies to access their account to perform a service, such as money management. It is also ties in to moves to require that bank accounts be portable, like cell phone numbers.[53] As it drives heightened connectedness and access, it is also helping to shift banking services onto a platform basis. For example, Starling Bank, one of the

[49] https://www.weforum.org/press/2017/08/big-tech-not-fintech-causing-greatest-disruption-to-banking-and-insurance/
[50] http://www.thesundaily.my/news/2017/06/29/tech-firms-overtake-traditional-banks-says-expert
[51] https://www.mckinsey.com/industries/financial-services/our-insights/data-sharing-and-open-banking
[52] https://www.wired.co.uk/article/open-banking-cma-psd2-explained
[53] https://www.finextra.com/blogposting/16281/understanding-bank-account-number-portability---psd2

"challenger banks" chartered in the UK to increase financial competition, uses its banking platform to help customers with non-financial activities.[54]

As discussed in Paper 3, the FCA issued a report in December 2019 seeking input on open banking and "open finance."[55] The paper emphasizes potential benefits to consumers, but also invites comments on potential problems.[56]

Open banking per se is less developed as public policy in the United States than in many other countries. Nevertheless, discussion is underway on both open banking and portability of accounts and data, and the U.S. is experiencing rising controversy over whether and how banks must allow fintechs to access accounts when a shared customer requests it.[57]

These emerging issues have the potential to bring major gains to consumers, but may also impact financial structures and introduce volatility into consumer behavior patterns, creating winners and losers among both incumbents and new entrants into the field.

Risks to the banking system may also arise as banks increasingly partner with fintechs and use them as vendors, in cases where new companies are not sufficiently stable, expert or secure.

Loss of confidence in the financial system

Another possibility is that consumers will lose trust in a new high-tech financial system that is immature, thereby stunting its potential. A catastrophic cyberattack or failure could do irreparable damage, as could increasingly widespread incidents of consumer harm. Manipulative and deceptive business models could chill fintech growth.

Consumers may also become leery of growing dishonesty and artificiality online. As they realize that seeming personal emails are coming from bots disguised as people, and as they worry about whether they are reading "fake news," significant numbers may turn away from online services and/or from

[54] https://podtail.com/fi/podcast/barefoot-innovation-podcast/digitally-native-finance-starling-bank-ceo-anne-bo/
[55] https://www.fca.org.uk/news/press-releases/fca-asks-proposals-how-open-finance-could-transform-financial-services
[56] https://www.fca.org.uk/news/speeches/open-finance-opportunity-financial-services
[57] https://www.cnbc.com/2019/12/16/venmo-and-pncs-fight-over-sharing-consumer-financial-data.html

providers that are not verified major brands. It is also possible that generalized concern about AI, especially in displacing jobs, will turn financial consumers against AI-enabled tools that could help them.

Cryptocurrency, crypto assets, and Libra:

Similar concerns arise regarding the expansion of cryptocurrency, including in peer-to-peer transactions. As discussed in Paper 3, the emergence of "stable coins" may bring a breakthrough in the popularity of using crypto for payments, as opposed to being speculative investments. This could raise a range of issues as to whether consumers fully understand these processes and how well they are regulated.

Such worries spiked sharply in 2019 when Facebook announced plans to issue, along with partners, a stable coin called Libra.[58] The innovation threw into relief the mismatch between current laws and regulatory structures versus mold-breaking innovation of this kind. At the federal government level, it was not even clear which agencies should play lead roles in regulating it. The ensuing controversy caused Libra's backers to defer some of their plans,[59] but it is fair to say that the episode served as a wakeup call regarding the gap between existing regulation and exponentially-changing financial technology.

A slightly earlier example of the novel challenges facing regulators was the sudden arrival several years ago of the Initial Coin Offering, or ICO, which uses cryptocurrency to raise funds in much the way an Initial Public Offering or IPO raises equity through stock sale. In June 2017, a startup called Bancor raised $153 million in two hours and twenty-five minutes. Gnosis raised $12 million in 15 minutes.[60] Regulators are not organized to respond quickly to innovations like these, which often strain or fall between their traditional domains, raise unprecedented issues, and involve large sums of money moving in a very short time. To enable desirable fintech to flourish, and to prevent new harm to the public, regulators will need new tools and new models – ones that, themselves, leverage the same technology that is transforming finance.

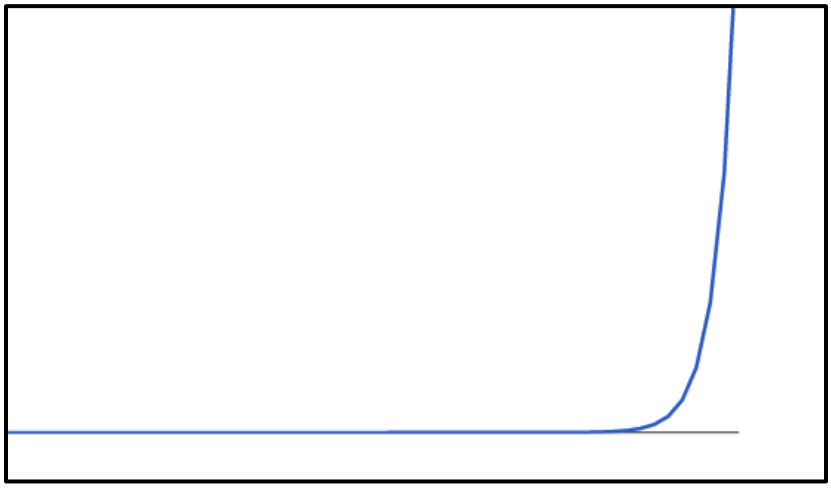
[58] https://libra.org/en-US/
[59] https://fortune.com/longform/facebook-libra-stablecoin-digital-currency-crypto/
[60] http://mashable.com/2017/06/18/ico-explained/#taizy01105qu

Pace and novelty of change:

As discussed extensively in Paper 3, an overarching problem is the pace of change itself, which will outstrip both consumer understanding and industry and regulatory readiness. In 1965 Gordon Moore posited Moore's Law, predicting that computing power would double every 18-24 months, a pattern that has largely held in the ensuing half-century.[61] A more recent IBM prediction suggests that the IoT will accelerate this to a doubling of global information every twelve hours.[62]

Futurist Niv Dror writes on the challenges arising as human brains and institutions that are wired for linear change try to cope with the exponential pace of technology growth.[63]

Figure 16



Source: Niv Dror, Medium, February 21, 2015

Risks Caused by Regtech

For most of the risks to consumers described above, it will fall to policymakers and regulators to fashion strategies to address them. Beyond this effort, they will also have to address new risks that will be raised by adoption of regtech, itself.

[61] www.mooreslaw.org/
[62] http://www.industrytap.com/knowledge-doubling-every-12-months-soon-to-be-every-12-hours/3950
[63] https://medium.com/@nivo0o0/when-exponential-technological-progress-becomes-our-reality-74acafd65e26

As discussed in Paper 4 in the Regulation Innovation series, there is clear evidence that the risks of *not* adopting regtech will outweigh the dangers of adopting it. Nevertheless, introducing digitally-native regtech will raise hazards and problems that will require substantial work. Again, solutions for these concerns will be covered mainly in the next paper, including the need for changes in regulatory cultures and skills.

The section below does not cover the obstacles to *use of* regtech, which were explored in the regtech Paper. Rather, this discussion focuses on problems likely to arise *because* of regtech.

Potential for failure:

The biggest driver of potential failure will be failure to move fast enough to address exponentially-changing technology.

At the same time, adopting these new regulatory tools will also bring risks. Intrinsic to adopting digitally-native regtech is the need to rely on digital technology. While this is a mature technology in many sectors, the providers of digital financial regtech are often young entities; the methods evolving in the space are, almost by definition, very new and relatively unseasoned. Regulators will have to fashion procedures and standards to assure that adoption is done right and to provide for the potential of individual companies in the space failing.

Unclear or shifting liability:

Some regulators are concerned that if they expand their real-time access to information about the companies they oversee, they might become subject to legal responsibility for problems they fail to detect and address. While this problem could arise today, digital connection with the industry could exacerbate it.

Misuse of data:

The previous section described the broad risk that will arise for consumers as more data is used and shared in the financial system. Regtech raises a related, specific concern about the possibility that increased regulator access to data could cause problems. If regtech produces centralized data repositories with individual consumer data, these could attract hackers. If regulators can more easily see information

on individual financial customers, some might abuse that power. It is also possible that regulators could misuse their access information about vulnerabilities of individual financial companies. Again, these kinds of risk exist already, but as with everything else, could escalate due to having more information easily and instantly available. Existing laws and policies may need to be revisited in crafting a digitized system.

Data quality risks:

Shifting to digital systems will require vastly more intake of data from both the regulated industry and external sources. Regulators will have to establish standards, processes and capacity to assure that data used in accurate and "clean," when used for purposes that require high quality.

The AI Challenge:

The previous section discussed risks to consumers arising from industry use of AI that could be either ineffective or biased, especially in areas like credit underwriting. Regulators will have to set standards and create oversight mechanisms to address this, in ways that can manage the "black box" problem described earlier. In addition, they will need to address the challenges that AI will bring to their own organizations.

As with industry AI, regulators will have to be able to verify that their own AI systems are designed in ways that verifiably produce meaningful and unbiased results. This will involve both setting design standards at the front end and building capability to audit results at the back end, even in situation where they may not be fully able to "explain" all the decisions that these systems are making.

In addition, as with other organizations, regulators will have to fashion new cultures and norms regarding the relationship between their people and their machines. Among other things, personnel will worry about having their jobs replaced. Agencies will have to design regtech systems that help their people and enhance their work, rather than undermining them.

In March of 2018 the Government Accountability Office issued a Technology Assessment entitled, "Artificial Intelligence: Emerging Opportunities, Challenges, and Implications,"[64] based in part on a forum it convened to explore AI issues in finance, criminal justice, cybersecurity, and autonomous vehicles.[65] The report noted that "…AI will have far-reaching effects on society—even if AI capabilities stopped advancing today" – which of course, they will not.

Bank of England Governor Mark Carney has said, "…utilizing ML and AI to analyse the data could free up supervisors' time to add the greatest value where human excel over machines: judgement."

Cloud risk:

Regulators will have to maintain sound standards not only for industry conversion to cloud computing, but also for their own. As discussed earlier, one risk will be the potential for systemic failure, since cloud services are currently provided by a small number of companies.

Risks to small banks:

Regtech has the potential to solve the regulatory problems of community banks facing disproportionate compliance costs and burden, as discussed in Paper 4. If mismanaged, however, it could make those problems worse. Community banks in general have low readiness for adopting digital technology. Most are contractually bound to traditional core processing companies that have limited capacity to effect rapid change. Some of these prevent or impede use of other technology vendors in concert with their systems. Some charge the bank for access to its own data.

In addition, regulators require banks to address "third-party risk" raised by using vendors. These standards, while necessary, are widely seen as creating regulatory risk around adoption of regtech solutions that do not have lengthy track records, which is, by definition, the case with true digital tools. These standards will have to be modernized, based on regulators' work on how to evaluate new regtech solutions. Regulators will need to facilitate an ecosystem conversion to regtech that works for community banks.

---

[64] https://www.gao.gov/products/GAO-18-142SP

[65] The author participated in this roundtable.

As fintech and regtech transform the system, most of the benefits and the problems discussed in this series are likely to emerge. Whether the good will ultimately outweigh the bad will depend heavily on how well this change is regulated. To regulate it well will require major changes.

The sixth and final paper in the Regulation Innovation series will explore what those changes should be, and will include discussion of practical strategies that could enable a full transition, over time.

Acknowledgments

I want to express my gratitude to Brigitte Madrian, Dean and Marriott Distinguished Professor in the Brigham Young University Marriott School of Business, for her mentorship in her previous role as Aetna Professor of Public Policy and Corporate Management at the Harvard Kennedy School. I'm also profoundly indebted to Amrita Vir for her invaluable contribution to this project as my research assistant at the Harvard Kennedy School.