The Crisis Next Time:
The Risk of New-Age Fintech and Last-Crisis Financial Regulation

Karen Petrou
Managing Partner
Federal Financial Analytics, Inc.*
info@fedfin.com
www.fedfin.com

September 6, 2018

Key Points

- Risk is risk regardless of legal charter unless risk-mitigation measures extend in like-kind ways to like-kind activities. This is not the case in key businesses conducted by banks versus non-banks. When the non-bank is also a fintech and then virtualizes risk, additional risks may well ensue because old ones remain and new ones – e.g., opacity, concentration – are injected.
- The FRB believes crisis risk is low due to all the new rules binding big banks. However, as finance moves outside banks and the infrastructure heads into the cloud, risk is quickly circumventing banking and threatening critical infrastructure, the ability of central banks to stabilize markets, and even the economic equality on which financial security depends.
- Although heavy-handed regulation suppresses innovation and efficiency, light-touch rules premised on the need to advance innovation and competitiveness have a dismal record of stoking financial crises, most recently in 2008.
- Near-term preventative measures are essential to prevent post-crisis, costly cleanup.

* This paper was prepared by Karen Petrou and FedFin without funding, input, or recommendations from any governmental agency or client. FedFin has private- and public-sector clients with varying interests on the questions discussed here, but the views represented are ours alone. In 2011, we issued the first paper – also ours alone – that identified the complexity risk of post-crisis regulation now the subject of extensive policy scrutiny. We hope that this fintech report spurs similar debate and do so more quickly so that there is no need to retrofit the regulatory framework after unintended effects manifest themselves in financial markets.

With the ten-year anniversary of the 2008 crisis upon us, a great deal of public attention is being devoted to identifying what or who caused it and whether new rules strike the right balance between prudence and macroeconomic growth. There is much to be learned, but one lesson stands out as a clear and immediate warning ahead of the certainty that financial markets will threaten another round of cataclysmic systemic risk: despite the months if not years leading up to the financial market's explosion in September of 2008, federal policy-makers were nonetheless dumbfounded and wholly ill-prepared when smoke turned to fire. Shortly before the debacle, Treasury Secretary Paulson assured us all was well. The Federal Reserve was equally convinced that Chairman Greenspan's "great moderation" and his stock-market "put" made financial crises a thing of the past. In his speech on August 24 of this year, Federal Reserve Chairman Powell said that he is confident that the U.S. is well-insulated from a crisis do-over thanks to all the new rules. Is financial stability really so much more assured now due to all the post-crisis rules and those still to come?

The purpose of this paper is to look for new signs of smoke, which I fear are already emerging not so much from the banking crater left by the last crisis into which the Fed still peers, but more ominously from new fintech mountains thrusting rapidly from the financial market's infrastructure in ways already redefining it with massive force and power. Given that financial technology (fintech) is almost entirely unregulated with regard to resilience, recovery, conflicts of interest, monopoly power, and pretty much everything else, this changing landscape poses significant risk from exactly the same vulnerabilities that sparked the last debacle and, even more worrisome, from new ones. As a recent paper observes, virtualizing financial risk by housing it in fintech companies does not change the fundamental nature of actual risk. Most tectonic shifts of this magnitude end in earthquakes.

In this short paper, I will show why technology regulation (TechReg)[1] should be developed before fintech falls prey to the profit-maximizing, short-term incentives that split the global economy asunder in 2008 when just one little sector – residential mortgages – exposed giant chasms of unrecognized, largely-unregulated risk. TechReg must be structurally different from finreg, but that financial technology is different from legacy banking does not make it less vulnerable to external threats and internal temptation. Indeed, as this paper will show, the absence of controls makes fintech risk not only different, but also already of immediate concern.

Amazon and Apple have now surpassed $1 trillion in market capitalization. Apple and Google also now control 99% of mobile phone software and the financial-market interfaces dependent on it. Public cloud computing is dominated by four companies that control 73 percent of the total market. The FRB conference at which Mr. Powell gave his remarks looked askance at all the competitive power concentrated in these firms, but largely only in terms of the issues at which central banks worry – i.e., monetary-policy transmission. Only passing thought was given to systemic risk, much as only a bit of worry was voiced about subprime mortgage finance until the financial system blew up.

This report[2] aims to sound an early warning where risks are already evident. It addresses:

- a capital- and operational-risk management construct for fintech essential to build sustainable business models across the business cycle and in the face of financial-market stress;

[1] Techreg is not "regtech." Regtech is generally meant to convey the use of artificial intelligence or other technology to speed compliance and enhance supervision and examination. In contrast, techreg here means fintech regulation.

[2] For brevity's sake, this report does not detail the factual assumptions underpinning our analysis. Important reviews may be found in papers from the Financial Stability Board [here, here, here, and here], Basel Committee [here and here], European Commission (here), European Banking Authority (here and here) and U.S. Treasury (here).

- safeguards against systems, underwriting, and governance opacity. Complex black-box operations increase the risk of conflicts of interest, credit or service-pricing discrimination, privacy breaches, inaccessibility for lower-income or disabled consumers, questionable risk management, and insider self-dealing. Risks of market disruption or even structural failure also increase;
- concentration-risk controls. The enormous clout Facebook, Google, Apple, and Amazon already exert in the mobile phone, cloud, and entire financial-product delivery and transaction infrastructure warrants upfront attention to avoid after-the-fact efforts to disentangle what global regulators fear could become natural monopolies or even oligopolies; and
- whether the known link between U.S. economic inequality and financial crises is tightened by market changes due to fintech activity.

Capital and Operational-Risk Management

An *a priori* difference between regulated finance and fintech is that banks – especially big ones – are under stringent capital, liquidity, and resolution protocols designed to put investor capital at first risk. One may dispute that these rules are tough enough, but at least there are rules. Fintech firms have no such requirements because it has long been assumed that, should one founder, its investors would take all the risk. However, given growing market reliance on fintech infrastructure and its increasing importance in bank-like product offerings, it is far from clear that the financial system, consumers, taxpayers, or even the macroeconomy are immune from fintech profit-maximizing behavior. It is thus already past time to consider where capital risk-alignment incentives and operational-risk buffers are required for fintech companies active in key financial arenas.

A critical question underpinning the regulatory construct that is still largely unanswered as fintech evolves is who owns or controls the use of consumer and customer data. Because of the rapid, successful evolution of large platform fintech companies, the fintech ecosystem is predicated on little to no privacy protections for consumer data housed outside regulated financial institutions. Recent privacy efforts in the European Union and other nations show the challenges and even risks of *post-hoc* efforts to redefine data ownership after unlimited use becomes a firm's or even an industry's *raison d'être*.

The need for action derives from the fact that, when customer data are used in ways that put capital at risk, an institution's self-protection incentives align – at least to some degree – with those of its customers because both take risk when privacy and proprietary data are breached. When a regulated financial provider with capital at risk owns customer personally-identifiable information (PII) or similarly-sensitive data, it has the resources with which to make good on fraudulent, data-breach, or similarly problematic transactions such as those for which current U.S. law assigns principal liability to the financial provider. In the event of large-scale disruption to a payment provider such as Venmo or to a non-bank payment service (e.g., Amazon), funds may be available for minor disruptions, but deep pockets for sustained losses are uncertain even at giant platform companies with no clear legal obligation to make customers whole in the event of system breaches or widespread infrastructure damage. The International Monetary Fund has recently estimated that financial-institution cyber-risk – now so grave it ranks as a systemic risk – ranges between ten and thirty percent of net income, a figure that takes into account only one type of operational risk in a sector under increasing attack from many quarters.

Even if a provider's solvency is not put at risk by making customers whole, the lack of clear legal responsibility to do so may well put vulnerable customers at significant risk, creating personal and even systemic harm. In 1974, a German bank, Herstatt, caused a global financial crisis due to lost foreign-exchange transaction capacity. In the Herstatt case, only foreign-exchange markets were at risk, but this

still meant grave danger to cross-border trade and market valuations. Slow cross-border technology at the time combined with governmental liquidity support saved the day. On September 11, 2001, a very different systemic risk – the World Trade Center attack – destroyed critical infrastructure. Market liquidity was then saved only by the largest injection prior to 2008 of Federal Reserve liquidity support to major U.S. banks and, thus, the global financial system. In these and other close calls with operational destruction, regulated banking survived largely due to capitalized resources and government support. Subject to lightening-strike operational risk, major fintech companies nonetheless have few capitalized resources and no right to FRB or other forms of federal liquidity assistance.

In addition to capitalized resources to absorb operational risks, banks and regulated exchanges are subject to extensive contingency-planning, redundancy, cyber-security, and even "living-will" requirements to ensure ongoing operations even under acute stress (e.g., the 9/11 attack, Hurricane Sandy). Major platform companies have indeed held firm under what is doubtless endless attack, but it remains unclear if their self-imposed standards are sufficient – the financial industry's never were, hence all the *post-hoc* regulations that toughen them up.

Reflecting these worries, bank regulators are quite concerned about operational-risk interfaces with fintech providers and resulting structural exposures. There is thus an increasing focus on applying bank-style resilience regulations to third-party service providers. However, the extent to which this occurs or can be enforced is uncertain. Further, even if third-party standards create *de facto* resilience requirements for fintechs, these may apply only in relation to transactions involving banks. Those operated by a fintech for the fintech and its non-bank customers remain outside scrutiny, capital requirements, or resilience testing.

Opacity

Proprietary, complex, model-driven, and often self-governing systems are a widespread concern across the spectrum of fintech operations from credit underwriting to cloud computing to mobile-payment delivery. And, as a recent draft report from Sen. Mark Warner (D-VA) found, many fintech business models are based on or offered in concert with services that offer free products (e.g., contact networks, search capacity) in return for rights to use data in ways (e.g., monitoring browsing to price credit) little understood and often undisclosed to consumers. Global and U.S. reports have highlighted at least some of these concerns, often focusing on the risk that fintech systems may use information gained from commercial transactions to "up-price" financial products or limit offerings in exclusionary or even discriminatory ways. However, few if any actions to date have countered these risks.

Reflecting these problems, Sen. Warner and others in Congress have proposed disclosures, opt-out rights and other protections so that consumers retake control of their PII. However, disclosures have long been an ineffective method to enhance consumer rights. "Information asymmetry" results from the length and complexity of most disclosures, especially those now required by law. Time and literacy constraints also limit disclosure impact, as do changing consumer needs and/or provider actions that can render any understood rights inapplicable to subsequent transactions. Users may also believe that they must obtain a service – i.e., a retail product or loan – and thus sacrifice PII or other proprietary information they would protect were alternative service providers available. "Dark patterns" (such as easy-to-trigger default options) also may trick users into disclosing considerably more information than suggested by any applicable disclosure about key terms and conditions.

To redress these limitations, one option would be to require that fintech providers take on obligations as "information fiduciaries." An "information fiduciary" would have duties akin to those well-

understood for financial fiduciaries – i.e., to use consumer information in the interest of the consumer, not for its own profit or other advantage known to be incompatible with the consumer's interest. A fiduciary duty is well-understood for financial-service providers, albeit controversial in connection with providing investment advice. Given the problems of disclosures in this arena, it is appropriate to evaluate the extent to which fiduciary duties should apply to the PII gathered directly when fintech accounts are opened, and when fintech-related PII is used to target advertising, alter commercial-good pricing, or otherwise affect the operations of the PII-holder not directly authorized by the consumer. Duties as an information fiduciary could also apply if PII is derived in the course of other transactions (e.g., messaging, personal postings) that is then used for fintech purposes.

Extending this information duty beyond the scope of financial products to which a fiduciary duty does not now apply (i.e., to offering loans or investment advice) is a complex undertaking, but one with considerable impact if accompanied by assumption of legal obligations. Firms that undertake an information fiduciary duty could also win greater market share as consumers grow increasingly wary of the ways in which PII is used. Such industry efforts were notably impressive when consumers began to fear the financial liability associated with debit-card use decades ago and banks voluntarily applied the same $50 limit to them as was applicable to credit cards.

Notably, U.S. bank holding companies are barred from "tying" traditional banking products sought by a customer (e.g., a loan) with a requirement or price incentive for the purchase also of an additional product (e.g., an insurance policy). As a result, knowing a lot about a bank customer makes it considerably more difficult to win market advantage. No such restraints apply to fintech companies unless they become known to the market and, even then, only if the Federal Trade Commission is willing or able to consider them unfair or deceptive acts or practices. In general, the only limitations governing use of PII pertain to privacy protection and recent history has shown those outside the regulated financial sector to be, at best, porous. Indeed, the FTC generally has only after-the-fact enforcement power, not the authority to issue rules that address cyber-security, consumer-protection, or privacy problems. Although the FTC's safeguard rule does establish minimum information security program standards for companies "significantly engaged" in financial activities, its definition of financial activities is narrow and its reach does not extend to financial activities conducted in firms such as all the giant platform companies – where fintech is only part of a broader corporate empire.

Banks are also required to keep careful documentation on and then to validate their underwriting and product-offering procedures. Absent any effort by the Bureau of Consumer Financial Protection to assert authority, no such examination or documentation requirements apply to fintech services, making it difficult to evaluate systems to determine if problematic outcomes are the result of market factors or illegal and improper actions.

All of these PII-protection and consumer standards create significant risks for consumers and market integrity. The asymmetry in the rules between banks and non-banks makes these risks even more problematic because banks may well exit certain businesses that on their face appear appealing to consumers – i.e., they are offered without charge – while non-bank companies deploy internal, often hidden techniques to profit from PII without the limits applicable to regulated companies.

Opacity also poses risk beyond PII use. While it is true that transparency and audit-ability slow down AI and ML, opacity in critical decision processes – e.g., credit provision, employment – provides essential protections not needed for small-dollar commercial transactions. Untrammelled business models may thus be considerably more problematic when platform companies go beyond current offerings to activities such as brokering stock sales, providing investment advice, lending funds on which small retailers depend, and supporting critical market infrastructure. Outside retail finance, opacity may also

protect trading strategies, investment models, and transaction-processing infrastructure in ways that add efficiency but also pose conflict-of-interest, resilience, market-correlation, and structural resilience problems. The inability of companies, let alone regulators, to validate and back-test AI/ML assumptions or to anticipate operational limitations in the third-party technology (e.g., mobile phones) upon which regulated-product delivery increasingly depends is also often mentioned by policy-makers as a significant fintech worry.

Reflecting all of these concerns, a recent U.K. trade association report proposes best practices to safeguard consumer, market, and policy interests. The idea here is to govern AI and ML fintech use through public statements and standards. New protocols could, this paper suggests, apply to privacy, conduct, cyber-resilience, and self-building or predictive-analytical models that may be ill-understood even by the companies that deploy them. It is unclear if such best practices would be pledges or if clear standards would be set by which firms could be held accountable through legal or other proceedings.

This report also addresses opacity challenges specific to cloud computing – e.g., requirements that regulated companies adhere to cloud-provider business practices and product parameters. Again, however, industry standards are also proposed as the solution to cloud-computing opacity and the different regulatory constraints that now limit bank use of this high-powered storage construct. The European Commission is currently working to construct such industry practices, but there is no such official effort underway in the U.S. beyond the concerns addressed by the U.S. Treasury report.

Given the uncertain value of best practices, self-regulatory organizations (SROs) might be a better approach to governing cloud-computing risk – the model has worked reasonably well in U.S. securities markets where prudential-regulatory authority does not apply. Interestingly, an effort supported to some extent by the U.S. Commodity Futures Trading Commission is underway to craft an SRO in the crypto-asset arena. However, creating an SRO for cloud computing or, indeed, other fintech activities would require not only far more cooperation than best-practice efforts have so far encountered, but also the force of law now granted securities SROs. Still, SROs go beyond setting aspirational standards along best-practice lines to set clear requirements and then enforce compliance with them. Fintech line-of-business SROs could, if granted this type of authority and then making use of it, thus make a meaningful difference.

Monopoly

Concentration risk is perhaps most acute when it comes to cloud service providers (CSPs). While not in any way limited to cloud computing, concentration is most acute here due to the small number of scaled providers and the critical importance of server capability. These attributes also raise stability risks due to the vulnerability of many institutions reliant on a single, potentially vulnerable CSP. Based on the systems threatened or even taken offline, interbank liquidity, ready access to payment, settlement, and clearing services, or other systemic risks could quickly manifest themselves. The ability of a central bank to intervene with liquidity support could also be threatened if it relies on the same CSP or its funding channels interact with it.

Regulators, including those in the U.S., are asking for information on cloud-outsourcing, but the value of these data remain uncertain based on varying formats and cross-border concerns. In the U.S., a CSP is arguably a third-party vendor to banks and thus subject to supervision; in practice, this has yet to occur and how it would is far from clear.

Cloud computing already has many characteristics of other core parts of the operational financial infrastructure (e.g., utilities). In sharp contrast to giant tech platform companies, these utilities are under extensive state regulation that is, while far from perfect, generally able to ensure service reliability, objective delivery at fair prices to all potential customers, and resilience under even acute stress. These non-CSP utilities are generally also inter-operable – that is, when one power company goes dark, nearby ones support customers and companies around the country rush in recovery and restoration services as needed.

The key to utility regulation is state-dictated pricing designed to ensure a reasonable return to value-oriented investors and dedication of earnings to system needs before capital distributions are allowed. Importantly, utilities are also generally limited in their permissible activities – i.e., they may not offer electricity and at the same time sell appliances due to potential conflicts of interest and business risks outside the reach of the utility-regulatory framework. Utilities also may not discriminate among customers – that is, even remote customers for whom service delivery is expensive must generally be served at the same price as those in more densely-populated areas.

Utility regulation for CSPs or any other infrastructure-critical fintech firm (including banks) in the U.S. would of course require new law, leading some – apparently including President Trump – to advocate an alternative that is subject only to administrative or market-driven efforts to invoke it: use of current antitrust law to break apart CSP or other monopolies (e.g., search engines, contact networks used for advertising and other commercial services).

Banks fall under very different rules limiting commercial or other non-banking activities to constrain market power, with these limits generally exempting them from antitrust regulation. Fintech platforms without activity and cross-selling restrictions in possession of troves of PII, and with no meaningful exposure to antitrust constraints are very powerful entities indeed, breaking through all of the limitations traditional in American practice to control structural market risk.

The challenge here, however, is that fintech and related infrastructure services are powerful precisely because of their scale. That is, without all of the data put to use to solve business problems or meet consumer needs, most platform-company offerings would be both less valuable and less useful. Significant economic-efficiency loss would thus ensue, as would like-kind efforts to force dominant hardware or software providers (e.g., Apple, Google) to release intellectual-property rights so that others could mobilize their now-proprietary technology. Like-kind risks at the very largest banks now are handled with regulation, not antitrust standards despite fears that these institutions are "too complex to manage." The scale of conflicts and complexity at even the largest banks is, though, no match for giant tech companies even as these firms are free of structural or regulatory controls.

Tech Power, Inequality, and Crisis Risk

As discussed above, giant tech companies already threaten to become natural monopolies or even oligopolies. This is of course a problem transcending financial regulation, but it warrants particular attention given the strong link between increasing economic inequality and greater vulnerability to another great financial crisis. A post on our ***Economic Equality*** blog points to a paper from the Federal Reserve Bank of San Francisco finding that, even if there isn't an asset-price bubble (usually seen as a crisis accelerant), economic inequality on its own not only stokes financial crises, but also is the best predictor that one is about to happen. This paper shows an historical correlation of inequality and crises across seventeen countries over the course of at least the fifty years preceding 2007. A more recent FRB staff paper looking solely at the U.S. concludes that the risk of secular stagnation, deflation, excess

credit growth, and financial crises increase in lock-step with income inequality, especially when interest rates are near the zero lower bound. How would giant tech companies make the inequality and crisis link still more inexorable?

They could. The risk here comes from rent-seeking – that is, the power of firms with few competitors exempt from utility-like regulation to do largely as they like in terms of product offerings, pricing, operational resilience, and corporate governance. A recent paper explores rent-seeking in detail with regard to giant platform companies, arguing that their ability to generate huge returns skews the overall economy to a small number of owners and high-skill workers compensated largely through capital income. The reasoning here is theoretical, but the fact remains that low-skilled workers – where there are any at platform companies – often struggle to earn enough to sustain even a modest living standard. The Federal Reserve conference referenced above considered this question along with the extent to which giant platform companies and their rent-seeking advantages undermine productivity, monetary-policy transmission, and other components of equality-enhancing financial policy, but it did not go on to economic equality. Interestingly, observers ranging from Sen. Bernie Sanders (I-VT) to Fox's Tucker Carlson have begun to do so.

It is indeed likely that the very success of U.S. tech companies and their contribution to overall GDP is very unequally shared. The more these companies exploit their market power – i.e., rent seek – the greater their ability to set wages instead of having to respond to them as competitive employers must. Low-skilled workers may thus find themselves in the wage trap already all too evident despite the recent "recovery." As a result, platform companies with monopoly or even oligopoly power may well increase inequality on their own regardless of their fintech operations, exacerbating crisis risk just by virtue of their enormous clout.

Further, large fintech operations in giant platform companies are likely also to exacerbate the inequality connection. This is because opacity and concentration may combine to deny credit and other forms of economic opportunity to those not favored by AI or ML models focused on profit maximization. The ability of platform companies to "micro-target" offerings or financial-product advertisements to selected groups is also of significant concern, as was most recently evident in a Department of Housing and Urban Development suit against Facebook alleging significant discrimination based on targeting housing advertisements to white and/or wealthy households. Online marketplace lending that uses credit-underwriting models based on factors such as university attended are also likely to have very disparate impact on lower-wealth borrowers, an issue of significant concern also for start-up small businesses given the critical importance of this activity to economic equality. The Treasury Department report referenced above details these concerns, albeit without proposing any solutions. The record of regulated banks providing banking services to minority populations, women, those with disabilities, and others not seen as high-profit customers is not without reproach. However, the transparency of bank underwriting models, the many regulators scrutinizing compliance, and the impact of the Community Reinvestment Act (CRA) all constrain the ability of banks to maximize profit at the expense of non-discriminatory product and service access.

Conclusion

With or without virtualization, risk is blind to the legal charter of the entity that takes it unless that legal charter comes with mandatory mitigation measures. Even then, though, risk may not only be mitigated, but also transformed in terms of consumer, macroeconomic, and financial-stability impact. When a business becomes uneconomic under one charter due to risk-mitigation requirements, the activity moves outside the regulatory perimeter if its economic rationale and profit benefits continue in the

broader financial-product marketplace. When that financial product is further transformed through application of AI, ML, or other virtualized processes, risk transformation resulting from regulatory arbitrage accelerates because, even though fundamental risk remains, it is obscured by opaque techniques. These may well be faster and smarter than legacy, book-driven procedures, but these benefits do not mitigate risk if speed and smarts are deployed to enhance firm profitability, not long-term safety and soundness.

Virtualized risk becomes still more dangerous when it transfers from many more or less competitive, regulated entities to a very few – or even just one – unregulated provider. When these very happy few govern critical aspects of financial-market infrastructure – i.e., through hardware dominance, cloud computing – risk grows still greater because one firm's profit-maximization incentives can make or break national or even global financial system.

Do we wait and see?