1

Key Threats to Financial Stability

In this chapter, we analyze three key vulnerabilities in the financial system today. Shocks that expose these vulnerabilities could disrupt the financial system and spread losses across firms and markets.

- **The financial system remains vulnerable to cybersecurity incidents, reflecting the financial sector's operational dependence on information technology.** Cybersecurity incidents rank near the top of our threat assessment because of the potential for disruption of operational and financial networks, and the damage such disruptions could cause to financial stability and to the broader economy. Cyber incidents can affect financial stability if defenses fail. We discuss ways to mitigate these risks.

- **New tools have been developed to make the orderly resolution of a failing systemically important financial institution more likely. Still, the failure of a large financial firm could amplify and transmit distress and possibly trigger a financial crisis.** Resolution under either U.S. bankruptcy law or a special resolution authority has potential weaknesses for handling global systemically important bank (G-SIB) failures in some scenarios. The treatment of derivatives of a failing financial firm continues to present a conundrum for policymakers seeking to balance contagion and run risks against moral hazard concerns. Also, tools for the orderly resolution of failing systemic nonbank financial firms remain less developed than those for banks, despite the material impacts of some nonbank failures in the past and the growing importance of nonbanks, particularly central counterparties (CCPs), in the financial system.

- **The evolving structure of some financial markets creates risks that need to be managed.** We discuss three risks. First, growing concentration in the provision of some key financial services means that sufficient substitutes may not exist if a dominant firm is unable to perform. Second, the increasing fragmentation of trading across multiple venues and products may limit the provision of liquidity in times of stress. Third, officials and market participants are well aware of the need to achieve a timely and smooth transition to a new reference rate to replace U.S. dollar LIBOR, which is now unsustainable. However, a disorderly transition could impair market functioning. LIBOR is an interest rate benchmark, formerly the London Interbank Offered Rate and now ICE LIBOR (Intercontinental Exchange LIBOR).

Note: All data cited in this report are as of Sept. 30, 2017, unless otherwise noted.

To identify these threats, we reviewed the wide range of risks that could potentially threaten financial stability. We weighed the potential impact, probability, proximity — could it happen soon? — and preparedness of private actors and the official sector. The top three threats, covered in this chapter, were the ones that scored high on these criteria. Lower-ranked risks are incorporated into our overall stability assessment in Chapter 2.

1.1 Vulnerabilities to Cybersecurity Incidents

The financial system is an attractive target for malicious cyber activity because it is interconnected and heavily reliant on technology. It handles trillions of dollars in transactions every day, which helps keep the economy moving. Sound risk management — including cyber hygiene — can protect firms in most cases from the many threat actors seeking to infiltrate or otherwise disrupt their operations. But some of these efforts will succeed. The likelihood and potential severity of cyber incidents continues to increase. We discuss how cyber incidents, like other operational risks, can disrupt financial firms if defenses and recovery efforts fail, which in turn could affect financial stability. We then discuss ways to mitigate the risks that an attempt will succeed and an incident will lead to financial instability.

The financial system, like other parts of the economy, is vulnerable to cyber incidents. Financial firms manage the wealth and handle the financial transactions that underlie the nation's economy. These roles attract malicious actors seeking to undermine confidence or to steal assets. They also mean that operational failures could cause costly disruptions of the financial system. The U.S. government has identified the financial services sector as part of the nation's critical infrastructure, with "assets, networks, and systems … that are vital to public confidence and the Nation's safety, prosperity, and well-being" (see White House, 2013).

In last year's *Financial Stability Report*, the OFR described how cybersecurity incidents at financial firms could threaten financial stability. We identified three possible channels: An incident could (1) disrupt the provision of key services, (2) reduce confidence in firms and markets, and (3) damage the integrity of key data. The Financial Stability Oversight Council (FSOC) has also recognized the systemic risks that cybersecurity threats pose (see FSOC, 2016).

Most cyber incidents fail. No incident has yet had systemic effects. But recent events — such as the hack of consumer information at Equifax and numerous intrusions against SWIFT customers — point to the potential risks. At the same time, several factors can increase the probability of an incident: the open structure of the Internet, the emergence of cryptocurrencies, and the legal liability of software developers. These factors can create risks for all companies, including financial firms.

Financial firms and regulators typically classify cybersecurity incidents as operational risk events. Many types of cyber incidents manifest themselves within a firm only where there is a breakdown of the operational risk management techniques the firm uses to increase its resilience in the face of such a failure. To limit the possibility that incidents occur within a firm and affect the stability of the financial system, the first step is to identify key vulnerabilities within the system, whether at the firm or system level. The next step is to work toward methods to manage such operational vulnerabilities. These techniques should be developed by the financial firms with assistance from regulators and other government organizations. They should be based upon a common lexicon and use common standards to improve the flow of information and operational risk management.

Where sound operational risk management is followed, including the development of strong response and recovery protocols, firms should be able to manage technology-related risks. Firms, however, may not always adequately weigh the costs of cybersecurity and other risk mitigation against the benefits. Typically, the costs of security are easier to measure than the benefits, which include benefits from breaches that do not succeed or reputations that are not ruined. Firms may also

decide that some types of threats are too costly to protect against, such as those originating from state actors or natural disasters.

How cyber incidents can affect financial stability

We describe five steps through which an attempt to disrupt information technology (IT) systems could create financial instability, if it is not successfully defended against (see **Figure 1**):

- **Cyber incident attempted.** Cyber incidents are deliberate efforts to disrupt IT systems to steal, alter, or destroy data. Threat actors have a variety of motives. Some seek profit. Others seek to disrupt governments or nations. Tactics are evolving. For example, there has been a recent increase in incidents involving use of ransomware (see Symantec, 2017).

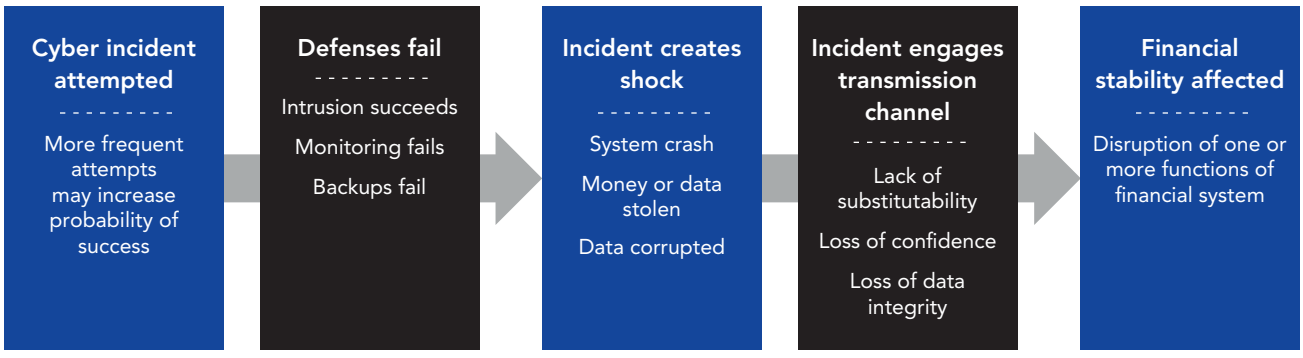
- **Cybersecurity defenses fail.** Cybersecurity encompasses the measures taken to protect a computer or computer system against unauthorized access or attack. Firms generally have multiple layers of defense. Many of the tools are based on operational risk principles regarding risk management and governance. A survey of developed-country financial regulators found that two-thirds, including most U.S. regulators, took a targeted approach to cybersecurity and IT risk in their regulations. The remaining one-third addressed cybersecurity as part of operational risk generally (see FSB, 2017a). Basic cybersecurity measures can mitigate up to 90 percent of threats by volume, according to financial company chief information security officers (see FSB, 2017b).

- **Threat actor succeeds; incident creates shock.** Threat actors succeed only in conjunction with operational failures: for example, monitoring systems that fail to identify a breach or threat, or recovery plans that do not quickly restore systems. No firm can be operationally perfect. Successful cyber incidents are shocks to the affected firms that cause, for example, system crashes, monetary losses, or data corruption.

- **Risks spread through transmission channels.** Whether a shock goes on to threaten financial stability depends on whether the incident engages the various transmission channels, as described below: a lack of substitutability, loss of confidence, or loss of data integrity.

- **Financial stability is affected.** The OFR defines financial stability as the condition in which the

Figure 1. How an Attempted Cyber Incident Could Affect Financial Stability



Source: OFR analysis

financial system is functioning sufficiently, even under stress, to perform its basic tasks for the economy. Those tasks are credit and liquidity provision, maturity transformation, risk transfer, price discovery, and the facilitation of payments.

Financial stability transmission channels

We rank cybersecurity incidents as one of the key threats to financial stability because, like other operational disruptions, such incidents could have systemic effects beyond the targeted firm or IT system. Where such an incident occurs, a customer or other financial firm may attempt to lessen the impact on their own operations by limiting exposure to malware or corrupt data that may emanate from the affected entity. Where insufficient workarounds exist, such a pullback might affect the normal operations of the financial system.

The OFR's *2016 Financial Stability Report* identified three channels through which cyber incidents can threaten financial stability, should a threat actor succeed:

Lack of substitutability for a key service or utility. In some financial markets, a few firms or financial market utilities serve as hubs, offering services that are difficult to replace if they are lost or interrupted. These hubs include central banks, custodian banks, and payment clearing and settlement systems. Without sufficient response and recovery plans at these entities, cyber incidents might disrupt the financial system's normal function.

To date, no malicious cybersecurity incident on a key financial hub has had systemic effects. However, operational disruptions have pointed to the potential for systemic risks. For example, in 1985, BNY Mellon, then the Bank of New York, received a $23 billion discount-window loan from the Federal Reserve to prevent a computer failure at the bank from spilling over to financial markets. That was a historically large loan at the time. The bank was one of only four institutions that cleared most Treasury securities trades. Its failure to provide such a critical service could have triggered a systemic risk event (see Ennis and Price, 2015).

Disruption of a key service provider can have rapid ripple effects. For example, in February 2017, an outage at Amazon's cloud computing service disrupted thousands of websites for four hours (see Hook, 2017). The outage was caused by an operational error during system maintenance, not a malicious cyber incident, and it did not involve a financial institution. Still, it showed the potential risks of relying on a single key provider (see Amazon, undated).

Loss of confidence among customers or market participants. Most cybersecurity incidents have been targeted and, as such, have had very little impact beyond the target itself. However, such an incident could trigger a broader loss of confidence. With good operational risk management in place, firms would review their own operational risk posture when an incident is announced elsewhere. Firms also would query firms in their supply chain to learn how well firms they rely on are protected against the same incident. Such practices could increase the resilience of the financial sector and the economy as a whole. Even an incident that affected only one firm could lead customers or market participants to question the defenses of similarly situated firms. Contagion through such channels is difficult to predict.

On Sept. 7, 2017, Equifax, the consumer credit reporting firm, said that hackers gained access to personal information for 145 million Americans, including Social Security and driver's license numbers (see Bernard and others, 2017; Cowley, 2017). The breach has not yet led to measurable changes in consumer behavior — unlike a similar event in South Korea in 2014, when consumers cancelled credit cards after a credit rating firm was compromised (see Sang-Hun, 2014). The Equifax breach did not cause financial instability, but led to a 35 percent drop in the firm's share price the following week. That loss of confidence appears to have induced a 16 percent drop in the share price of TransUnion, the largest U.S. competitor to Equifax. The third major credit bureau, Experian, is a subsidiary of a British firm whose stock price fell about 5 percent that week. Neither TransUnion nor Experian reported breaches.

Loss of data integrity. The integrity of financial data is critical to the functioning of financial institutions and markets (see OFR, 2016). Financial firms need robust backup data. However, tradeoffs exist between recovering quickly and ensuring that recovered data are safe, accurate, and do not spread cyber risks, especially for markets that process orders rapidly. A data corruption event could disrupt market activities or functioning.

It is difficult to know in advance exactly what will cause a cyber incident to be transmitted through one of these channels and destabilize the financial system. How large or important must an institution or network be so that a lack of substitutability causes a systemic problem? What type of incident will cause a loss of confidence so great that it causes customers to flee from an affected firm and its peers? In what scenario will data corruption cripple a market? For each of these channels, is there a cumulative effect, or a tipping point where customers and counterparties lose confidence? Further research is needed to evaluate these questions.

Factors increasing the odds of cyber incidents

In **Figure 1**, the arrows through black boxes represent the escalation of a threat. The first black box illustrates how an intrusion can bypass defenses to become a successful incident. The second illustrates how an incident can spread through transmission channels to affect financial stability. We present them as black boxes because little is known today about the likelihood of escalation at that point and how that escalation would occur.

At the OFR, we are concerned about factors that increase the chances that a cyber intrusion will affect financial stability. Those black boxes make it hard to tell directly what the probability of instability will be. But we can look at factors that increase the number of attempts. More attempts increase the probability of an incident that could affect financial stability, especially as threat actors refine their attacks based upon evolving understanding of the potential victim.

Here we explore three examples of factors that could increase the probability of an incident: the open structure of the Internet, the emergence of cryptocurrencies, and the legal liability of software developers. These factors are not unique or specific to financial firms. They are also not under the immediate oversight of financial regulators. However, they can create risks for financial firms and the financial system.

Open structure of the Internet. The Internet was designed with an open structure to foster communication among disparate computer networks. That communication has brought great benefits to users. Internet-related activities contributed 4 percent to 7 percent of U.S. gross domestic product (GDP) between 2011 and 2016. But the Internet's open structure has increased opportunities for malicious acts and thus the risk of a damaging incident. A single incident launched via the Internet can affect many firms at the same time, in many countries, or spread quickly from one firm to the next. Annual U.S. cyber losses totaled 0.1 to 1.3 percent of U.S. GDP between 2011 and 2016 (see Kopp, Kaffenberger, and Wilson, 2017).

Assaults can come from overseas and from state-sponsored actors. The WannaCry ransomware incident in 2017 hit firms in more than 150 countries. The affected firms were mostly outside the financial sector. Still, a similar incident that breaches the defenses of multiple financial firms could trigger market reactions and threaten financial stability.

Cyber infiltrators can work from foreign jurisdictions that can't or won't curtail their activities. The potential payoffs of cross-border cyber crimes are relatively high, while the risks of arrest and prosecution are relatively low. Recent research concluded that a 10 percent increase in the number of Internet users globally is associated with an 8 percent increase in the number of Distributed Denial-of-Service (DDoS) incidents. In a DDoS event, bad actors bombard a site with access requests, blocking legitimate Internet users (see Overvest and Straathof, 2015).

Emergence of cryptocurrencies. Cryptocurrencies — encrypted digital currencies — can increase the incentive to conduct malicious cyber activity. Off-shore

Industry and Regulatory Preparedness

Cyber incidents can threaten financial stability through three channels: lack of substitutability, loss of confidence, and loss of data integrity (see OFR, 2016). Firms and regulators continue to invest in information security. They collaborate in sharing information to defend IT networks and in protecting data to improve resilience.

Federal bank regulators have existing supervisory programs that contain general expectations for cybersecurity practices at financial institutions and third-party providers. In October 2016, the bank regulators proposed enhanced cyber risk management standards to be integrated into the existing programs, in an advance notice of proposed rulemaking (see Board of Governors, OCC, and FDIC, 2016). The proposed rule has not been issued.

Other U.S. financial regulators continue to develop cybersecurity standards. The National Association of Insurance Commissioners in October 2017 adopted a model law for protecting insurance data. Data protection is a key concern for insurers in light of several cybersecurity incidents targeting health insurance data. Insurers, like other financial institutions, are required under regulations implementing the Gramm-Leach-Bliley Act of 1999 to safeguard certain sensitive customer data. The model law is a significant step forward, but still awaits adoption by U.S. states.

The Federal Housing Finance Agency (FHFA) issued new guidance on information security management in September 2017, which supersedes previous guidance on cyber risk management. The newly published guidance provides high-level standards covering areas such as risk assessment, network and software security, data classification and protection, and incident response and recovery, but does not prescribe specific standards or technology solutions. Bank regulators have the authority to examine third-party service providers, including information technology and other critical service providers. The FSOC has recommended in its annual reports that similar examination and enforcement powers be granted to the FHFA, as well as the National Credit Union Administration.

Other gaps remain. For example, there is an absence of regulatory guidance on management of cybersecurity risks by consumer credit reporting companies. This gap was highlighted by the recent breach of Equifax, which may have exposed the credit records of nearly half of all Americans. These types of incidents could pose a financial stability risk if there is a loss of confidence in financial institutions or in the integrity of consumer financial data.

Firms also collaborate with each other and with government agencies to share information about cyber risks and to build resilience. For example, Sheltered Harbor, a nonprofit industry initiative, is expected to launch in late 2017. Institutions that join Sheltered Harbor agree to store encrypted copies of their customers' data in their own air-gapped, immutable, and survivable "data vaults" in a specified industry standard format. The initial focus is on U.S. retail banks and brokers.

The Financial Services – Information Sharing and Analysis Center, which sponsored Sheltered Harbor, also established the Financial Systemic Analysis and Resilience Center (FSARC) (see OFR, 2017a). FSARC's members include 14 large banks and utilities that work with U.S. regulatory, intelligence, and law enforcement agencies to identify and assess cybersecurity threats to critical financial infrastructure.

trading of cryptocurrencies makes it easier for criminals to move and hold funds pseudonymously and evade detection. Before cryptocurrencies, cybercriminals using ransomware relied on payment vouchers to extort money from victims. Off-shore trading venues for cryptocurrencies provide a means to transfer funds outside the traditional financial system (see Symantec, 2016). One security firm estimated there were 463,000 detected ransomware incidents in 2016, up 36 percent from 2015 (see Symantec, 2017).

Use of cryptocurrencies is minuscule today in proportion to traditional payment methods. However, that use has grown rapidly. The estimated value of cryptocurrencies topped $100 billion in the summer of 2017, as prices rose. Bitcoin, the best-known cryptocurrency, accounted for almost half the outstanding value (see Vlastelica, 2017). For perspective, total U.S. financial assets exceeded $90 trillion as of June 2017 (see Board of Governors, 2017a).

Regulators have moved to make use of cryptocurrencies less alluring. In the United States, on-shore trading venues for cryptocurrencies are subject to federal money transmission and anti-money laundering laws (see FinCEN, 2013). Overseas, Australia and Japan recently adopted new laws, recognizing Bitcoin as legal tender and expanding their supervision of cryptocurrencies, including the imposition of money laundering regulations (see Smyth, 2017). The further development and international adoption of such rules may reduce the ease of off-shore trading of cryptocurrencies for illicit purposes, including cyber threats.

Legal liability for software development. Software flaws can increase the probability of cyber incidents because malicious actors can exploit them to enter a system, or to cause damage once an intrusion occurs. A defect in widely used software can open the door to widespread disruptions. The legal treatment of software defects may contribute to this situation. Financial firms should develop a robust operational risk methodology to minimize the externalities imposed by IT vendors.

Most manufactured products are subject to product liability laws. These laws give manufacturers an incentive to ensure their products are safe and reliable. But software developers are not generally subject to U.S. product liability requirements (see Sales, 2013). Software developers are usually considered service providers, not product manufacturers, under U.S. law (see Butler, 2017). Software is often licensed under usage agreements that limit liability, rather than being sold outright as a product. This treatment provides first-mover incentives that promote rapid software innovation, sometimes at the expense of security.

Firms should defend against this risk by testing their systems and planning for recovery. To date, the standards for software testing by manufacturers and users are voluntary (see ISO, 2013).

How to mitigate the risk that an attempt succeeds

The nature of cybersecurity incidents continues to evolve, demanding a robust and flexible response from the private and public sectors (see **Industry and Regulatory Preparedness**).

In the United States, many financial and nonfinancial firms use the National Institute of Standards and Technology (NIST) Cybersecurity Framework as a starting point for managing cybersecurity risk. In a May 2017 executive order, the President instructed executive branch departments and agencies to adopt that framework (see White House, 2017). The NIST framework describes core cybersecurity activities:

- *Identify* critical systems, assets, data, and capabilities that are vulnerable.
- *Protect* those systems to ensure delivery of critical infrastructure services.
- *Detect* cybersecurity events as they occur.
- *Respond* when a cybersecurity event has been detected.
- *Recover* any capabilities or services that were impaired because of a cybersecurity event.

The NIST framework calls on firms, among other things, to have an overall cybersecurity strategy; to have a chief information security officer in charge of IT security; and to set security standards for third-party service providers. Financial regulators rely on the NIST framework and on international supervisory guidance for cyber risk management (see NIST, 2014; CPMI-IOSCO, 2016).

It is impossible to prevent all cyber incidents. This is why firms use multiple layers of defense, sometimes called defense-in-depth strategies. Such strategies aim to make it more difficult for a failure of one defense to lead to a breach. However, such systems can be costly. Firms must weigh how an incident would affect earnings, assets, and reputation. The costs of putting in place protective measures are known and measurable, but the benefits of preventing incidents are harder to evaluate. Too little is known about the probability and potential severity of different types of intrusions. A firm's board of directors should consider these factors and make these decisions as part of its risk management framework.

A main concern for policymakers is that the orderly operation of the financial system is a public good. If one firm is unable or unwilling to take actions needed to protect a critical operational component, the effects could be felt far beyond the firm.

Conclusion

Financial firms, no matter where they are within the financial system, work to defend themselves against cyber incidents. They also work to build resilience. Research that helps financial firms and regulators address questions about the channels that transmit stress will support system-wide resilience. How do we measure costs and benefits to improve the tradeoff and ensure spending is effective? How do we better assess the probability and severity of cyber defenses failing? How do we measure success? What government resources should be spent to protect the public good that is financial stability, as firms themselves lack the incentive and ability to secure the financial system?

The OFR has a two-pronged approach to researching cybersecurity and other operational risks. In the first prong, we review event studies, recent experiences, and other information to understand past events involving financial entities and how they might threaten the financial system. We evaluate current regulations and gaps in policy that could affect the financial system's resilience. We draw lessons from tabletop exercises, which bring together financial firms and regulators to examine potential scenarios.

The second prong of OFR research applies network analysis to potential cybersecurity risks and other operational risks. The OFR has broad authority to collect data from federal financial regulators and market participants. This authority allows the OFR to analyze detailed transaction-level datasets. We are using these data to develop maps that highlight connections throughout the financial sector. These maps will help us identify key vulnerabilities and critical institutions across different markets.

Network analysis identifies the most critical firms in the market. This analysis offers several key lessons for improving defenses. One lesson is that a network's resilience can vary greatly against different types of threats. Targeted attacks by sophisticated adversaries can cause much more damage than random failures, and these attacks call for a much higher level of network resilience. Another lesson is that coordinating defense strategies among network participants is vital in preventing weaknesses in defense systems. A lack of coordination between market participants and regulators can compromise network stability and leave key institutions under-defended.

1.2 Resolution Risks at Systemically Important Financial Institutions

The failure of a large financial firm could amplify and transmit distress, and possibly trigger a financial crisis. Since the 2007-09 crisis, new tools have been developed to make the orderly resolution of a failing systemically important financial institution (SIFI) more likely. However, resolution under either U.S. bankruptcy law or a special resolution authority has potential weaknesses for handling global systemically important bank (G-SIB) failures in some scenarios. The treatment of derivatives held by a failing financial firm continues to present a conundrum for policymakers seeking to balance contagion and run risks against moral hazard concerns. Tools for orderly resolution of failing systemic nonbank financial firms remain less developed than for banks, despite the material impact of some nonbank failures in the past and the growing importance of nonbanks, particularly central counterparties (CCPs), in the financial system.

The Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank Act) establishes two paths for the resolution of a failing SIFI. First, it seeks to make orderly resolution through bankruptcy more plausible. Second, it provides the Treasury Secretary the authority to place a financial firm into Federal Deposit Insurance Corp. (FDIC) receivership, upon the recommendation of federal banking regulators and in consultation with the President. This Orderly Liquidation Authority (OLA) under Title II of Dodd-Frank is meant, in part, to address concerns about financial stability and improve cross-border coordination of a resolution among regulators. OLA acts as a backstop to the bankruptcy process.

Some of the key actions taken to assist resolution through either bankruptcy or OLA include:

- **The Dodd-Frank Act introduced a "living will" requirement.** It requires bank holding companies with assets of $50 billion or more and nonbanks designated by the FSOC for Federal Reserve supervision to submit resolution plans to the Federal Reserve and the FDIC. The U.S. G-SIBs currently submit these plans every two years. Each living will describes the company's strategy for a rapid and orderly resolution in bankruptcy. The effectiveness of OLA and bankruptcy depends on the viability of these living wills. The G-SIBs submitted their most recent plans in July 2017. The Federal Reserve and the FDIC currently are reviewing these submissions.

- **The FDIC led the development of a single-point-of-entry resolution strategy in the United States.** This strategy allows the top-tier holding company of a SIFI to enter resolution via bankruptcy or a Title II receivership while its material legal entities remain in operation. Seven of the eight G-SIBs have adopted this strategy in their living wills.

- **Bank regulators' 2017 living will guidance advises that G-SIBs are expected to estimate and hold sufficient resources for an orderly resolution.** To support the bankruptcy strategies in their living wills, U.S. G-SIBs are expected starting in 2017 to estimate the capital and liquidity that each material legal entity within the firm would need in a resolution, and

to pre-position sufficient resources between the parent and material legal entities accordingly. These expectations, however, are not requirements. This advance positioning of resources is essential to the single-point-of-entry resolution strategies of most G-SIBs. Moving resources among legal entities after resolution could face legal challenges from creditors whose interests are affected by those moves.

- **The Federal Reserve introduced a total loss-absorbing capacity requirement.** It requires U.S. G-SIBs and U.S. intermediate holding companies of foreign G-SIBs to maintain a minimum level of total loss-absorbing capacity and long-term debt to absorb losses or recapitalize these firms' material legal entities as part of the firm's resolution process (see Board of Governors, 2016). The final rule for this requirement was issued in late 2016 and will be effective at the start of 2019.

- **The International Swaps and Derivatives Association (ISDA) developed the qualified financial contract (QFC) stay protocol to address issues raised by regulators.** QFCs are statutorily defined to include derivatives, repurchase agreements, securities lending transactions, and certain other bilateral contracts. In bankruptcy, creditors of a failing firm typically must observe an automatic stay on all claims. A stay prevents creditors from collecting money the debtor owes. However, QFCs generally are exempt from stays under bankruptcy law.

  The Federal Reserve and the FDIC recently issued final rules requiring G-SIBs and their subsidiaries to amend their QFCs in a manner consistent with the ISDA 2015 Universal Resolution Stay Protocol (see Board of Governors, 2017b; FDIC, 2017a). The Office of the Comptroller of the Currency (OCC) is expected to issue a final rule shortly. The protocol opens a short window of between one and two days during which counterparties to G-SIB QFCs cannot terminate those positions. This time period would allow transfer of these obligations to a third party, preserving the value of the assets and the orderly functioning of markets. Following a successful resolution, counterparties would no longer have cause for termination.

  However, the rule applies only to U.S. G-SIBs and the U.S. operations of foreign G-SIBs, not to other banks or nonbank financial firms. Additionally, the stay does not apply to G-SIBs' centrally cleared derivatives with central counterparties. Central counterparties can continue to take risk mitigation measures towards a failing G-SIB clearing member, such as requiring additional margin or even terminating a G-SIB's centrally cleared positions.

These developments go a long way toward making orderly resolution tenable under bankruptcy or OLA. However, there are still scenarios in which a G-SIB resolution through bankruptcy or OLA may not achieve their intended outcomes.

Remaining G-SIB Resolution Risks

One scenario that may challenge the new framework would involve multiple G-SIB failures at the same time. It is doubtful that more than one G-SIB could be restructured and released from FDIC oversight — much less be wound down — quickly enough to stabilize the U.S. financial system. Handling multiple OLA interventions at the same time would present substantial resource and planning challenges for authorities. Another scenario would involve a G-SIB failure in the midst of a market crisis that is more severe than anticipated. Many of the failure scenarios and the subsequent exit strategies assume a failing bank can dispose of some of its business lines to raise funds while operating other business lines. But market strains could hinder asset disposition strategies.

New Federal Reserve and FDIC guidance on estimating and maintaining pre-positioned liquidity at

material legal entities and the total loss-absorbing capacity rulemaking create the possibility that a G-SIB could fund its own bankruptcy. However, no failing large bank or financial firm has ever self-funded its own resolution in bankruptcy before. For this reason, the Dodd-Frank Act also establishes OLA to allow U.S. regulators to act outside bankruptcy to ensure the orderly resolution of a systemic firm with an official-sector liquidity backstop. It is possible, for example, that the pre-positioned resources prove insufficient in stress and additional official sector resources would be needed to support the continuing operations of material legal entities.

There have been some legislative proposals to strengthen the bankruptcy code's provisions for financial firms and eliminate OLA. However, significant obstacles to the orderly resolution of a G-SIB via bankruptcy remain. Potential obstacles to orderly resolution in bankruptcy include insufficient liquidity, pre-failure planning, governance preparation, and international coordination. The treatment of derivatives in bankruptcy also could be improved to reduce the risks of resolving large portfolios. For these reasons, OLA remains an essential tool.

Resolution Risks Posed by Derivatives Portfolios Involve Trade-offs

Resolving nonbank financial firms' over-the-counter (OTC) derivatives positions via bankruptcy remains challenging. There is no set of policy options that can guarantee an orderly G-SIB resolution through bankruptcy. For this reason, OLA remains a crucial backstop.

The current U.S. Bankruptcy Code was created by the Bankruptcy Reform Act of 1978. Under the code, a debtor has the court's protection against creditors in the form of an automatic stay (see U.S. Bankruptcy Code, 2010). This stay allows the bankrupt entity to work out debts while preventing some short-term creditors from exercising their claims against the firm (see Hance, 2008). Should this fail, the stay allows the receiver to liquidate assets and repay creditors.

However, over time, exemptions to the stay provision have been added to the bankruptcy code and expanded to prevent a systemic collapse should a derivatives counterparty be unable to liquidate its contracts with a bankrupt debtor immediately (see Morrison and Edwards, 2005). The exemptions, known as safe harbor provisions, cover derivatives, repurchase agreements, securities lending transactions, and certain other bilateral contracts. The safe harbor provisions allow creditors to close out these contracts even after a firm has filed for bankruptcy. This exemption from bankruptcy's stay was intended to reduce contagion risk — that is, the risk of spillovers to a failing firm's counterparties that could spark a broader crisis.

> Historically, there have been problems with resolving nonbank financial firms' over-the-counter (OTC) derivatives positions via bankruptcy.

In 1998, the Federal Reserve organized a private consortium of creditors of Long-Term Capital Management L.P. (LTCM) to buy and manage the wind-down of the failed firm's derivatives portfolio. A key concern was the potential for spillovers from a LTCM default to its derivatives counterparties (see Morrison and Edwards, 2005). This concern contributed to the expansion in 2005 of the exemption from the bankruptcy law's automatic stay to a broader range of QFCs to include essentially all derivatives contracts (see Roe, 2011; Simkovic, 2009). Some researchers have argued that the exemptions may have reduced monitoring of the creditworthiness of OTC derivatives' counterparties, encouraging greater derivatives use (see Roe, 2011; Simkovic, 2009). The exemption, however, also gave rise to a different systemic risk: the risk of runs by a bankrupt firm's derivatives counterparties (see Morrison and Edwards, 2005). When Lehman Brothers Holdings Inc. filed for bankruptcy in September 2008, that's what happened. Derivatives did not cause Lehman's failure.

But terminations by Lehman's counterparties resulted in losses on its derivatives portfolio and magnified the impact of its failure on the financial system.

Counterparties terminated most of Lehman's more than 6,000 derivatives contracts, covering more than 900,000 transactions. Those terminations were complex and expensive because it was difficult to determine their final values. The valuation problems, in turn, came about because derivatives markets were overwhelmed by attempts by Lehman's counterparties to terminate existing contracts with Lehman and negotiate new contracts with new counterparties to replace the terminated contracts. At the time, Lehman's derivatives holdings accounted for about 5 percent of the global market and its resolution was disruptive. The Lehman estate spent about $40 billion to terminate swaps alone (see Roe and Adams, 2015).

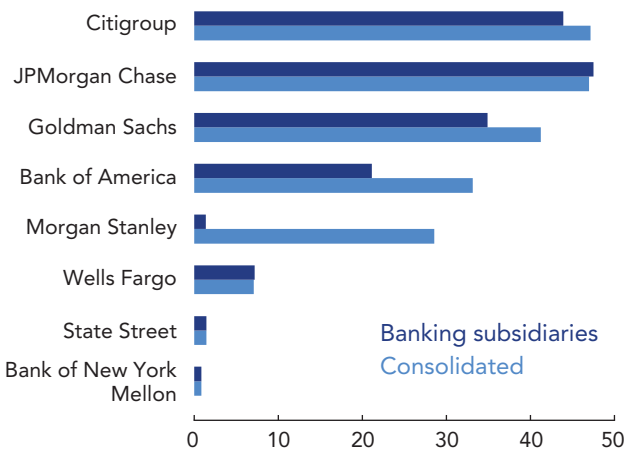
The terminations also disrupted short-term funding and derivatives markets in the weeks after Lehman filed for bankruptcy (see Fleming and Sarkar, 2014). Markets were further disrupted by concerns about the impact on Lehman's counterparties despite the exemption from the automatic stay.

Since the Lehman failure, changes to U.S. bankruptcy law have been proposed to partially roll back QFC exemptions to stays in light of the experience during the financial crisis (see Lee, 2015; Roe and Adams, 2015). Other proposed changes would specifically address financial firms. Some of the proposals to amend the bankruptcy code may increase the possibility that a U.S. G-SIB could be resolved through bankruptcy. Some proposals would also eliminate OLA as a backstop to bankruptcy. However, OLA is an important tool, capable of addressing the potential obstacles to bankruptcy discussed in the previous section.

Most U.S. G-SIBs' derivatives holdings are in banking subsidiaries that would be subject to the FDIC's resolution authority regardless of potential changes in OLA or bankruptcy law. Still, there are three U.S. G-SIBs — Bank of America Corp., Goldman Sachs Group Inc., and Morgan Stanley — with significant derivatives holdings in their nonbank subsidiaries; if OLA were eliminated, these nonbank subsidiaries could potentially be resolved through bankruptcy rather than an FDIC receivership (see **Figure 2**). So if OLA were eliminated, there are cases in which the resolution of material derivatives portfolios of a G-SIB's nonbank affiliates would occur through bankruptcy. This could be problematic if these nonbank affiliates need official sector liquidity support during bankruptcy. Specifically, a G-SIB's OTC derivatives counterparties could still terminate contracts if they did not receive required timely variation margin payments during the bankruptcy.

Figure 2. U.S. G-SIB Banking Subsidiaries' Gross Notional Derivatives ($ trillions)

Derivatives are mostly held in banking subsidiaries



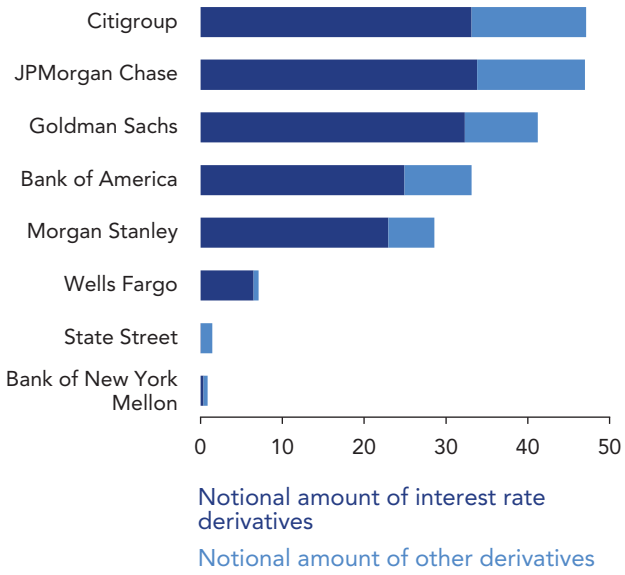
Note: Data as of Dec. 31, 2016. G-SIB stands for global systemically important bank. Differences in reporting can cause subsidiary totals to exceed consolidated amounts.

Source: Federal Reserve Form Y-9C, Federal Financial Institutions Examination Council Call Reports, OFR analysis

Although the ISDA protocol provides for a two-day stay on G-SIBs' bilateral OTC derivatives, there have been proposals for further changes to QFC exemptions from stay under U.S. bankruptcy law. Some proposals call for reestablishing longer stays (see Lee, 2015; Roe and Adams, 2015). Increasing the length of a stay would give the debtor more time to find potential assignees or obtain needed liquidity. But no matter the time period, finding assignees for a larger U.S. G-SIB's OTC derivatives portfolio could be difficult. Other proposals call for assigning derivatives portfolios to multiple firms by

Figure 3. U.S. G-SIB Derivatives Holdings ($ trillions)

Interest rate derivatives make up bulk of portfolios



Note: Data as of Dec. 31, 2016. G-SIB stands for global systemically important bank.

Source: Federal Reserve Form Y-9C

breaking up portfolios by product lines or counterparties (see Lee, 2015; Roe and Adams, 2015). But if a portfolio consists mostly of one type of derivative or of transactions with a single counterparty, the sub-portfolio could still be too large for most potential buyers (see **Figure 3**). This would imply that a wind-down of a failed G-SIB's derivative positions would require a number of months.

Disposing of derivatives portfolios in a bankruptcy creates other problems. If the derivatives portfolio is deeply out of the money, selling the failed firm's portfolio might not be possible. The larger the portfolio, the bigger the challenge. A deeply out-of-the-money derivatives portfolio would need to be transferred with cash, which a failed firm would likely lack. Additionally, a longer stay could raise questions about who would hedge and manage the risk of the portfolio before an assignment.

What the effects of some of the new resolution tools will be on a G-SIB's derivative counterparties is also unclear. These new tools require bank holding companies to maintain sufficient capital and liquidity to ensure that material subsidiaries remain operational. These resources must be backstopped by top-level holding company unsecured long-term debt and equity available to absorb additional losses. But these requirements could create moral hazard and reduce incentives for counterparties in OTC derivatives transactions with G-SIBs to monitor their risks. The ISDA protocol and related rulemakings could be expected to incentivize firms to find ways to innovate in response to the stay and limits on termination post-bankruptcy.

In sum, challenges remain in balancing the systemic risks of contagion, runs, and moral hazard while crafting policy responses for the legal treatment of a financial firm's derivatives in bankruptcy.

Although $483 trillion in OTC derivatives still traded globally as of year-end 2016, the Dodd-Frank Act provisions mandate standardized derivatives transactions move to central clearing (see BIS, 2017). As noted, G-SIBs' centrally cleared derivatives are exempt from the ISDA stay, and CCPs could terminate these G-SIB derivative positions even earlier. The expansion of derivative CCPs poses its own resolution challenges.

Tools for Orderly Resolution of Systemic Nonbank Financial Firms Remain Less Developed Than for Banks

The Dodd-Frank Act has increased the centrality of some nonbank financial institutions in U.S. financial markets, especially CCPs. CCPs benefit markets, promoting efficiency and reducing counterparty credit risk. They also concentrate credit risk in the CCP itself (see OFR, 2017b). A distressed CCP could impose losses on its clearing members, which include all G-SIBs. For this reason, Moody's Investors Service, Inc., a rating agency, explicitly incorporates expectations of public sector support in its ratings of CCPs (see Moody's, 2017). The U.S. Department of the Treasury recently noted that regulators should seek to prevent taxpayer-funded bailouts and limit moral hazard by addressing the systemic

risks posed by CCPs and other financial market utilities (see Treasury, 2017).

Planning for a potential failure of a systemically important CCP differs from that of the U.S. G-SIBs. CCPs are not subject to the living will requirements of the Dodd-Frank Act, including capital and liquidity requirements or limits on growth or divestures that can be imposed if regulators determine that the resolution plans are not credible. However, CCPs are required to develop recovery and orderly wind-down plans to address extreme circumstances that could threaten the CCP's viability and financial strength before the point of insolvency is reached. CCPs designated as systemically important that are primarily regulated by the Commodity Futures Trading Commission (CFTC) have drafted initial recovery and orderly wind-down plans. After a preliminary review, the CFTC issued guidance in 2016 requiring more detailed planning for a minimum of eight potential business and operational risk scenarios. However, unlike the living will process for G-SIBs, which has deadlines and associated sanctions, the CFTC guidance does not specify an effective date. Designated CCPs primarily regulated by the Securities and Exchange Commission must complete their initial plans by the end of 2017 (see SEC, 2017c).

Even with these plans, there is a lack of clarity about how a CCP failure, however unlikely, could be executed. By statute, CCPs must be liquidated via Chapter 7 of the bankruptcy code. Potential options, such as a substitute CCP, might permit continuity of critical functions, which could help avoid the termination of the CCP's positions and allow for an orderly wind-down of the operations of the failed CCP. However, substitutability could be a problem because some products are only cleared at present by one CCP; even where multiple CCPs clear the same products, there can be differences in clearing member rules and margin requirements. Absent a substitute, the alternatives could be the termination of the positions at a failed CCP or government support to the CCP. Terminating a CCP's positions would likely cause market turmoil.

In addition to CCPs, there are other nonbank financial firms that could be systemically important by virtue of their size, complexity, or interconnections with G-SIBs and other SIFIs. For example, some of the largest insurance companies have extensive financial connections to U.S. G-SIBs through derivatives. For some insurers, evaluating these connections using public filings is difficult. Insurance holding companies report their total derivatives contracts in consolidated Generally Accepted Accounting Principles (GAAP) filings. Insurers are required to report more extensive details on the derivatives contracts of their insurance company subsidiaries in statutory filings, including data on individual counterparties and derivative contract type. But derivatives can also be held in other affiliates not subject to these statutory disclosures, resulting in substantially less information about some affiliates' derivatives than required in insurers' statutory filings (see **Figure 4**).

OLA can be invoked in the case of an insurance company under Title II. However, in most cases state resolution mechanisms are expected to operate. State insurance supervisors only have the authority to resolve insurance company subsidiaries domiciled in their state with court approval. Other non-insurance affiliates that may be integral to the operations or risk management of the holding company would fall outside of insurance regulators' jurisdiction. An insurer's foreign affiliates also would be subject to other insolvency proceedings.

Figure 4. Consolidated vs. Statutory Derivatives Reports for U.S. Insurers ($ billions)

Company	Consolidated GAAP	Statutory filings	Difference
American International Group, Inc.	181	101	80
Ameriprise Financial, Inc.	142	137	5
Hartford Financial Services Group, Inc.	56	37	19
Lincoln National Corp.	105	101	4
MetLife, Inc.	418	325	93
Prudential Financial, Inc.	366	169	197
Voya Financial, Inc.	113	103	9

Note: Data as of Dec. 31, 2016. GAAP stands for Generally Accepted Accounting Principles.

Sources: SEC Form 10-K, SNL Financial LC

Conclusion

There are a range of new policy tools to help resolve SIFIs. These tools have narrowed G-SIB resolution risks considerably. However, the simultaneous failure of multiple G-SIBs remains a concern. Also, while self-funded bankruptcies for G-SIBs are now more feasible, OLA remains a critical backstop. The treatment of derivatives of a failing financial firm under bankruptcy continues to present a conundrum for policymakers seeking to balance contagion and run risks against moral hazard concerns. Resolution planning could be more developed for systemically important nonbank financial firms.

1.3 Evolving Market Structure

Financial markets evolve in response to financial disruptions, regulatory changes, and new technologies and business models. This section looks at three aspects of market structure that could create vulnerabilities: the lack of substitutability for essential services; the fragmentation of trading activities across multiple venues and products; and the transition to a new reference rate to replace LIBOR.

A market's structure is defined by the number and types of participants; ease of entry; participants' information, influence over price, and business models; the evolution of business models; trade execution; and regulations and laws. Financial market structure is also affected by crises and corrections. As market structures evolve, the financial system may grow more resilient to stress in some ways but more vulnerable in others. For example, the OFR has focused in previous reports on the growing role of CCPs in derivatives markets. CCPs reduce counterparty exposures between financial firms but concentrate risk in the CCP (see OFR, 2017b).

This section describes three facets of evolving market structure that may create vulnerabilities. First, some markets depend on one or a few financial institutions whose services may be difficult to replace under stress. Second, trading in some markets is fragmented across many venues or products. This fragmentation introduces risks in rebalancing liquidity provisioning and harmonizing prices. Third, market participants are preparing to switch from LIBOR to a new reference rate. The new rate promises to be more robust and reliable. But failure to achieve a timely and smooth transition could impair market functioning.

Lack of Substitutability

Well-functioning financial markets are essential to capital formation and economic growth. The execution and completion of a financial transaction often involves service providers that specialize in different steps of a transaction, such as order placement, trade execution, and payment and settlement.

The provision of these services can be concentrated in a small number of firms. For example, concentration occurs when economies of scale drive marginal costs to zero, creating natural monopolies, which is common in markets for heavily automated services. Concentration also arises from major market participants creating functional utilities to solve a collective industry concern. The concentrated provision of services can be optimal for market efficiency. However, concentration brings with it greater risks from the failure of the key service provider because of a lack of substitutes to fill the void. The inability of a natural monopoly, or functional utility, to operate, particularly in periods of stress, could lead to a breakdown in liquidity and in the market's ability to fulfill its price discovery role. Such a breakdown could spread to other markets through price effects or fire sales by individual firms experiencing losses.

Here, we discuss two examples of markets that depend on service providers to perform key functions. First, we look at growing substitutability concerns in the settlement of U.S. Treasury securities and related repurchase agreements. The heavy reliance by many firms on a single institution for settlement of these trades is a key vulnerability. A break in settlement services by this provider could affect liquidity in the Treasury market and disrupt other markets that rely on Treasuries for pricing and funding. Second, we examine the more complex structure of U.S. equity markets, which have historically faced a number of substitutability risks. In equity markets, service providers have developed several operating practices to mitigate the systemic failures that could be caused if a service were to fail. Equity markets, however, are similar to other markets that have many stages in the

processing of transactions. Many of those stages can be vulnerable because of a lack of substitutes. Policymaker attention to evolving market structures and the creation of new single points of failure is needed.

Policymaker attention to evolving market structures and the creation of new single points of failure is needed.

Lack of substitutability in the settlement of Treasury securities and related repos

The Treasury market will soon be more dependent on a single bank for the settlement of Treasury securities and related repos. A service disruption, such as an operational risk incident or even the bank's failure, could impair the liquidity and functioning of these markets because some customers will need time to move their operations elsewhere. It could also disrupt other markets that rely on Treasuries for pricing and funding. The 2007-09 financial crisis showed the damage that can be done if activity in short-term funding markets is constrained.

Dealers in Treasury securities use clearing banks to settle Treasury cash transactions. Since the 1990s, these services have been provided by two clearing banks, JPMorgan Chase & Co. and Bank of New York Mellon Corp. (BNY Mellon). With JP Morgan Chase's announcement in July 2016 that it intends to cease provision of government securities settlement services to broker-dealer clients, this business will be concentrated in a single bank.

A disruption in BNY Mellon's Treasury settlement could have broad implications for the Treasury market. It could disrupt trading in Treasuries. If settlement services were interrupted for an extended period, risks could spread further to markets that rely on the Treasury market for hedging and pricing.

While rare, operational issues have caused disruptions in the past. In November 1985, a computer problem prevented the Bank of New York (the predecessor to BNY Mellon) from delivering Treasuries, forcing it to borrow from the Federal Reserve Bank of New York to finance the securities. The Sept. 11, 2001, terrorist attacks severely disrupted BNY Mellon's connectivity. These disruptions prevented the Government Securities Clearing Corp., now the Fixed Income Clearing Corporation (FICC), from providing BNY Mellon with delivery instructions. A shortage of Treasury collateral and increased settlement fails lasted for weeks, despite action by the Federal Reserve to lend its own Treasury securities. The shortage was not alleviated until the Treasury Department conducted an unscheduled reopening of the on-the-run 10-year note on Oct. 4.

JPMorgan Chase and BNY Mellon are also the two banks that clear triparty repo transactions. A repo allows a firm to sell a security to another firm while promising to buy it back at a later date. In a triparty repo, a third party (the clearing bank) provides clearing and settlement services. The triparty repo market is a key source of funding for large banks and other financial firms. As part of its exit from government securities settlement, JPMorgan Chase plans to stop settling transactions for triparty repos using Treasuries as collateral soon. JPMorgan Chase's departure from the market will leave BNY Mellon as the sole provider of these settlement services. FICC's General Collateral Finance repo service also depends on BNY Mellon for settlement.

A disruption in services could have broad implications in the market for triparty repos backed by Treasuries. Triparty repo borrowers could have to scramble for alternative funding sources or reduce leverage, potentially creating a liquidity squeeze and fire sales. Reference rates in the future will increasingly be based on Treasury repo markets. Disruptions in repo markets could affect liquidity and prices in the cash market for Treasury securities. The implementation of monetary policy could also be affected because the Federal Reserve relies on triparty repo settlement to manage its reverse repo facility, which the Federal Reserve uses to put a floor under the federal funds rate.

To be sure, measures that regulators and market participants have taken since the global financial crisis have

improved the resilience of the triparty repo platform and its participants. Banking reform now de facto requires stronger leverage and liquidity positions for broker-dealer affiliates of bank holding companies, many of whom are major triparty repo borrowers. Settlement practices have been revamped to reduce the extension of intraday credit by the triparty settlement banks but operational dependence remains.

Lack of substitutability in U.S. equity markets

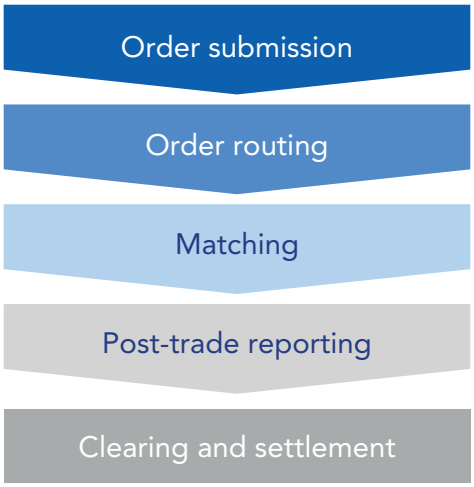
U.S. financial markets have seen growth in the number of trading venues, and with that growth, more points where a lack of substitutes could pose a threat. Market infrastructure disruptions paired with periods of financial distress can have systemic risk implications. Here we discuss how these issues have appeared in U.S. equities markets.

As the number of equity trading venues has increased, service providers that act as functional utilities have arisen to integrate the complex market structure. Under stress, the inability of these providers to participate in the market could disrupt equity market functioning and also spread to other financial markets, including options and futures markets. Concerns about similar potential ripple effects led the Federal Reserve to provide liquidity to banks after the 1987 stock market crash (see Carlson, 2006). Today, these functional utilities have developed operational risk controls and mitigation techniques. However, across the different stages of an equity's transaction that these providers serve, risk remains.

The key stages in the life cycle of an equity trade are: (1) order submission, (2) order routing for best execution, (3) matching, (4) post-trade reporting, and (5) clearing and settlement (see **Figure 5**). A lack of substitutability at any step in the trade life cycle may disrupt the market's ability to provide key services such as price discovery and liquidity.

After an order is submitted, it is routed. Typically, a broker-dealer attempts to internally fulfill the order to reduce costs. If internal fulfillment is not possible, the dealer routes the order to an exchange, wholesaler, or dark pool that can fulfill the order at the lowest execution cost. Dark pools are private trading venues where

Figure 5. Life Cycle of an Equity Trade



Source: OFR analysis

traders anonymously buy and sell securities. In deciding where to route the order, pretrade quote information is accessed to determine where best execution can be achieved. The listing exchange's securities information processor (SIP) collects, processes, and disseminates the information in a single, consolidated, and easily consumed data feed to determine national-best-bid-and-offer quotations. Although other avenues exist for disseminating prices, there is only one official SIP for each major listing exchange.

Nasdaq halted trading for three hours in August 2013 because of a technical glitch in its SIP. Technical glitches, which have been widely reported in the media, result in marketwide trading halts that can impair price discovery and liquidity provision. These events also create confusion among market participants in the form of busted trades. A busted trade, for example, could be one that is executed at the wrong price due to a SIP malfunction. There are no marketwide rules for resolving such problems. To address the risks posed by these potential single points of failure, Nasdaq and the New York Stock Exchange (NYSE) have built backup facilities and hardware to increase resilience and reliability. They have also improved their capacity and scalability.

Once an order is routed to a venue, the venue's matching engine is responsible for matching orders and

executing trades. A malfunction of that engine can cause trade and pricing to be misaligned. Typically, this is not a problem because there are several trading venues. However, in the case of opening and closing prices, the listing exchanges are the only venues determining these prices. These prices are particularly important because they are also used to establish prices for futures and options. The matching engine at the NYSE, one of the listing exchanges, failed in November 2012 and July 2015. Equity trading ceased briefly on the NYSE while trading continued on other exchanges. The NYSE and Nasdaq have since agreed to back each other up during technology malfunctions that hinder the daily closing auction. In addition, in the event neither firm is able to perform the closing auction, they have agreed on a last-resort methodology, known as the volume-weighted average price.

Once a trade is executed, the trade information is transmitted to the SIP to help inform future trade routing and determine the national best bid and offer. In the case of off-exchange trading venues, post-trade information must first be sent to a trade reporting facility, which then sends the information to the SIP. In August 2015, the trade reporting facility run by Nasdaq and used by off-exchange venues experienced a brief outage, affecting roughly 30 percent of trade volume. A more extended outage could have caused broader disruptions, as regulators require off-exchange venues to halt trading when such outages occur. Since then, the Financial Industry Regulatory Authority (FINRA) has issued guidance that allows firms to continue trading if they have a backup reporting facility. Otherwise, the firms must shut down trading in the event of a widespread systems outage (see FINRA, 2016).

In the last stage of an equity transaction, the trade is cleared and settled. Clearing and settlement ensures sellers are paid for the securities sold and buyers receive the securities purchased. Centralized clearing and settlement provides efficiencies by reducing transaction costs and improving liquidity for clearing members. Central clearing allows market participants to deal with the clearinghouse rather than with many separate counterparties.

In equities markets, one major clearinghouse, National Securities Clearing Corp. (NSCC), guarantees the completion of transactions. If NSCC's clearing system malfunctions, a bottleneck of unsettled trades could occur, which would create uncertainty about firms' actual positions. This single point of failure could be another risk to financial stability due to a lack of substitutability in the life cycle of equities trades. NSCC recently introduced an operational risk management methodology to assess critical functions and a technology risk management group to develop business continuity plans (see SEC, 2017b).

Automation and evolving market structures

Financial markets will continue to evolve to meet customer demand and exploit technological innovations. For example, financial market use of blockchain, a digital ledger technology that records transactions, is in its infancy. Although the expectation is that blockchain will simplify settlement services, its full implications for financial market structures are yet unknown. Blockchain and the ongoing automation of transaction processing could cause new single points of failure to arise naturally. Regulators and market participants should watch for these new points of failure and create suitable resiliency plans.

Even in equity markets, where steps have been taken to increase market resilience if a dominant service provider fails to perform, vigilance is needed. New single points of failure can arise as market structure evolves. The risk from a market's reliance operationally on a single firm often is not recognized until trading processes are halted by problems at the firm. Ongoing operational risk management by such firms and industry-wide business continuity planning are essential.

Market Fragmentation

The presence of multiple service providers can mitigate to some extent concerns about a lack of substitutability. It creates natural substitutes, drives competition, and incentivizes innovation. Healthy competition across providers can also promote diversity in the provision

of specialized services. All these factors can reduce systemic risks.

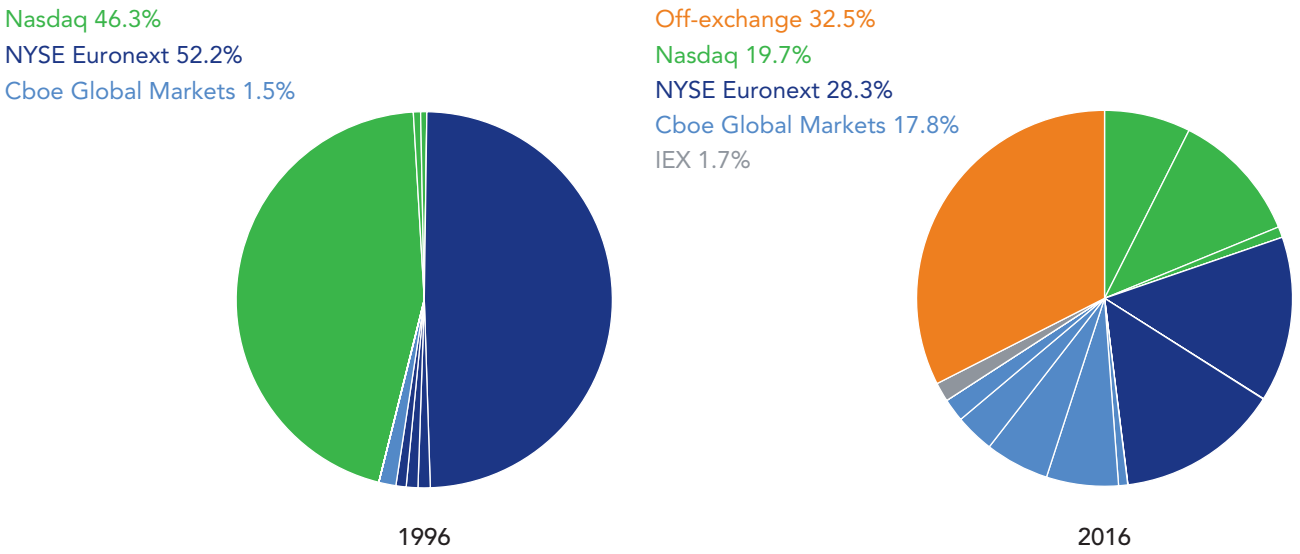
But different issues can plague markets with many service providers. Market fragmentation can increase, and with it, the market's complexity. Fragmentation also reduces the transparency of how a transaction occurs. Both of these factors can increase overhead costs to end users, particularly during periods of stress. For example, the number of electronic exchanges available for equity trading has grown substantially, most notably in equities (see **Figure 6**). The availability of multiple trading channels has been beneficial because it provides flexibility for risk managers desiring to hedge portfolios and for corporate treasurers and portfolio managers who want to reallocate assets quickly under stress. Healthy competition across exchanges has helped these markets avoid the single-point-of-failure and substitutability concerns discussed previously.

However, fragmentation of trading activity across many exchanges splits price discovery and reduces market liquidity (see Gresse, 2017; Upson and Van Ness, 2017). Price discovery and liquidity depend on well-capitalized players who can buy when prices are depressed by investor flight. Fewer market makers now operate, and their resources are stretched thin across an ever-increasing number of exchanges and products. Market makers have had to spend more to stay fully connected across venues because trading speed is crucial for them to remain competitive and manage their market risk. The added costs and reduced profits for firms that supply liquidity have led these firms to consolidate. In a stress event, if several of these large participants stop market-making activities, many markets could fail to efficiently price securities, simultaneously slowing or halting trading. Firms serving other venues could be less able to fill the gap if they lack trading relationships. This is one channel through which increased market fragmentation increases financial market vulnerabilities.

Moreover, the rapid-fire shifting of liquidity across many trading venues can help generate contagion during episodes of market stress, as firms may not be able to access liquidity in other segments of the market.

Figure 6. Market Share by Exchange, 1996 and 2016 (percent)

The exchange landscape has shifted notably



Note: Cboe Global Markets, Inc., Nasdaq, Inc., and NYSE Euronext, Inc., are holding companies, each with multiple stock exchanges. The shaded slices in 1996 and 2016 represent exchanges that they run now. In 2016, there were more than 50 off-exchange markets.

Sources: Muzan Trade and Quote

Recent research examining the fragmentation of equities markets also suggests that the operation of dark pools can draw order flow away from "lit" exchanges, reducing liquidity in the latter. In lit markets, the limit order book is publicly displayed; in dark pools, it is not (see Degryse, de Jong, and van Kervel, 2015). Illiquidity itself can be self-reinforcing by discouraging investor participation. In a flight to quality, dealers may have trouble finding counterparties or liquid trading venues to adjust their inventories.

Some markets are also becoming more fragmented across products, raising concerns that the availability of liquidity may also become more fragmented. With markets fragmented by product, there are fewer dealers participating in any given market. Those dealers, constrained by their own position limits, may be unable to respond to increased customer demands, particularly when liquidity has dried up under stress. How these risk channels would play out in a crisis is unknown and remains an area of debate among regulators and academics. The concentration among market makers may correct itself over time as more nonbanks enter the market (see Duffie, 2012).

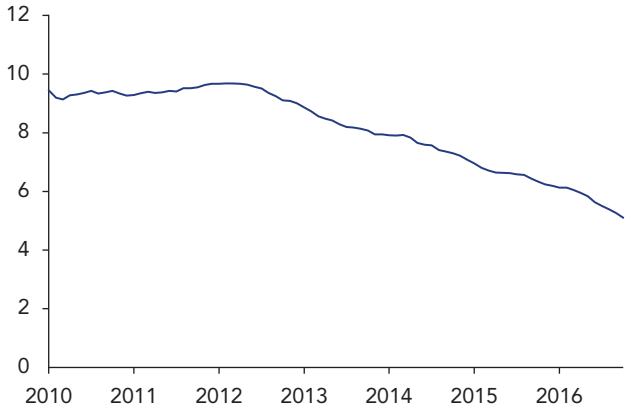
Fragmentation concerns have centered on OTC markets for fixed-income securities. Changes in banking regulation may have affected bank-affiliated broker-dealers' behavior in ways that could harm market liquidity during times of stress. Traditionally, OTC markets have had a core-periphery market structure with a larger number of investors buying and selling products through a core set of dealers that intermediate trades for the periphery. This arrangement drives trading activity to larger dealers, most of which are bank holding company affiliates. There are tradeoffs to this market structure. On the one hand, there are benefits to concentration — sharing the fixed costs of inventory management, position margining, and product expertise. On the other hand, there are benefits to fragmentation — interdealer competition, diversified product research, and substitutability.

Studies have shown that corporate bond market liquidity has now recovered to precrisis levels (see Adrian and others, 2017; Anderson and Stulz, 2017; SEC, 2017a). At the same time, there is evidence that some banking regulation has disincentivized bank-affiliated dealer liquidity provision in fixed-income markets. For example, one Federal Reserve paper looked at the effects of the Volcker rule, which limits proprietary trading by banks. The authors found that bank-affiliated dealers subject to the rule have reduced their market-making activities, ceding business to dealers not affiliated with banks (see Bao, O'Hara, and Zhou, 2016).

OFR researchers found that the implementation of the Volcker rule coincided with dealers specializing in serving particular segments of the single-name credit default swap (CDS) market, decreasing the number of market makers for any one CDS product (see **Figure 7**). An earlier OFR working paper showed that significant losses suffered by a large dealer that was central to several niche markets could have contagion effects, because capital constraints could bind and affect all the product segments the dealer serves (see Siriwardane, 2015).

Figure 7. Dealers in U.S. Single-Name Credit Default Swaps (number)

Average monthly dealer participation per CDS reference entity



Note: Data as of October 2016.

Source: OFR analysis, which uses data provided to the OFR by the Depository Trust & Clearing Corp.

Reference Rates

Firm price-setting behavior is a key feature of a market's structure. In markets for loans and debt securities, firms typically set interest rates based on a reference rate. For many years, U.S. dollar LIBOR has been the primary reference rate for syndicated commercial loans and interest rate derivatives in U.S. markets. Interest payments on at least $10 trillion in credit obligations and more than $150 trillion in the notional value of derivatives contracts were linked to U.S. dollar LIBOR at the end of 2013.

But LIBOR is unsustainable across a number of currencies. It is based on a survey of a shrinking pool of market participants and reflects transactions in a shrinking market. Most LIBOR survey submissions are based on judgment rather than actual trades, and the rate tracks unsecured transactions, which represent a small share of banks' wholesale funding.

To replace LIBOR, alternative reference rates are being identified across global markets via an initiative coordinated through the Financial Stability Board, an international group of financial authorities (see **Figure 8**). The alternatives selected so far include both secured and unsecured rates. All are based on higher volumes of transactions with overnight tenors that reflect minimal credit risk.

In the United States, the Alternative Reference Rates Committee (ARRC), largely made up of banks active in the derivatives market, in June announced its choice of an overnight Treasury repo rate as an alternative to LIBOR. The new rate, called the Secured Overnight Financing Rate (SOFR), will be produced by the Federal Reserve Bank of New York, in cooperation with the OFR. The SOFR will be based on robust trading activity in repos backed by Treasury securities, not on bank surveys. The rate as initially conceived will use data on repos backed by Treasury securities from the

Figure 8. Properties of Selected Rates

	Area	Currency	Rate	Credit Risk	Onshore	Most-transacted underlying tenors
Old Regime	United States	Dollar	LIBOR	Yes	No	3-Month
	United Kingdom	Pound sterling	LIBOR	Yes	Yes	3-Month
	European Union	Euro	EURIBOR	Yes	Yes	3-Month
	Japan	Yen	LIBOR, TIBOR	Yes	No, Both	3/6-Month
	Switzerland	Franc	LIBOR	Yes	No	3/6-Month
New Regime	United States	Dollar	SOFR	Near-risk-free	Yes	Overnight
	United Kingdom	Pound sterling	SONIA	Minimal	Yes	Overnight
	European Union	Euro	EONIA	Minimal	Yes	Overnight
	Japan	Yen	TONAR	Near-risk-free	Yes	Overnight
	Switzerland	Franc	SARON	Near-risk-free	Yes	Overnight

Note: Decisions for Switzerland and the European Union are tentative. LIBOR stands for London Interbank Offered Rate. EURIBOR stands for Euro Interbank Offered Rate. TIBOR stands for Tokyo Interbank Offered Rate. SOFR stands for Secured Overnight Financing Rate. SONIA stands for Sterling Overnight Index Average. EONIA stands for Euro Over Night Index Average. TONAR stands for Tokyo Overnight Average Rate. SARON stands for Swiss Average Rate Overnight.

Source: OFR analysis

triparty repo market and from two segments of the repo market in which trades are conducted through a central counterparty.

Policymakers and market participants are taking steps to affect a smooth transition to an alternative rate. Much work remains in the next few years to complete the process. Still, the failure to achieve a timely and smooth transition to a new reference rate could impair the functioning of markets that now rely on LIBOR. There are two main channels through which problems could occur.

First, banks' submissions to the LIBOR survey could continue to drop, but not below the minimum number needed to continue publication of LIBOR. If that happens, survey results may poorly reflect changes in the funding environment. Consequently, it would become difficult to use derivatives markets to hedge risks, because derivatives depend on reference rates to accurately reflect relevant economic trends. If this occurred, the financial intermediation capacity of institutions reliant on these markets could be impaired.

Second, LIBOR publication could be discontinued before market participants agree to new benchmarks for existing contracts. U.K authorities, who regulate LIBOR, have taken steps to maintain the pool of survey participants until the end of 2021 and cannot guarantee publication after that point (see Bailey, 2017). Legacy contracts that use LIBOR often lack robust provisions for calculating payments in the event that LIBOR is discontinued. To minimize this problem, all new contracts and amended legacy contracts must identify fallbacks that are robust and that limit unintended valuation changes (see Powell, 2017). Contracts that roll over regularly will be easier to amend than those for longer-term bonds. Most contracts have provisions for selecting fallback rates if the stated reference rate is no longer available. Implementing this provision could be more challenging for some contracts, such as collateralized loan obligations, that require all bondholders to approve such a change.

These concerns are heightened by the short time available for transition before LIBOR publication is no longer guaranteed. The Federal Reserve Bank of New York plans to begin publishing the new rate daily in the first half of 2018, leaving three to four years for derivatives markets referencing the new rate to develop.

LIBOR is deeply embedded in the financial system, but the challenges have been identified for many years, and industry and government are working cooperatively to address them.

Conclusion

Policymakers and financial firms need to continue to track structural changes in how markets work. These changes may make markets operate more efficiently and create opportunities for new business models that better serve customers. But changes in market structure can also create new vulnerabilities. Three consequences of evolving market structures that may present financial stability risks demand particular attention in the coming years. First, natural monopolies or functional market utilities that provide essential services can be single points of failure. Second, the fragmentation of equity trading across venues and products can split price discovery and reduce market liquidity. Third, failure to achieve a timely and smooth transition to a new reference rate could impair the functioning of markets that now rely on LIBOR.