MOODY'S ANALYTICS

ANALYSIS
JANUARY 2024

Cyberattack Contagion in the Financial System

Cyberattacks pose a growing threat to the global financial system, with recent breaches exposing vulnerabilities deep in its plumbing. Given the rapid digitization of the financial sector and proliferation of cyber threats, the prospect of a cyber event with far-reaching consequences for economic and financial stability is a serious risk.

This paper considers two adverse cyberattack scenarios on the U.S. financial system. We use the Moody's Analytics Global Macroeconomic Model to trace the channels and economic consequences of each attack. The first scenario considers the economic fallout of a deposit run, precipitated by successive cyberattacks on small and medium-size financial institutions. The second scenario explores a cyberattack that paralyzes the retail payments system. Though differing in timing and magnitude, the economic damage in each scenario is meaningful.

Prepared by

Jesse Rogers
Jesse.Rogers@moodys.com
Assistant Director\Economist

Matt Colyar
Matt.Colyar@moodys.com
Economist

Mark Zandi
Mark.Zandi@moodys.com
Chief Economist

Contact Us

Email
helpeconomy@moodys.com

U.S./Canada
+1.866.275.3266

EMEA
+44.20.7772.5454 (London)
+420.234.747.505 (Prague)

Asia/Pacific
+852.3551.3077

All Others
+1.610.235.5299

Web
www.economy.com
www.moodysanalytics.com

Cyberattack Contagion in the Financial System

BY JESSE ROGERS, MATT COLYAR AND MARK ZANDI

Cyberattacks pose a growing threat to the global financial system, with recent breaches exposing vulnerabilities deep in its plumbing. Given the rapid digitization of the financial sector and proliferation of cyber threats, the prospect of a cyber event with far-reaching consequences for economic and financial stability is a serious risk.

This paper considers two adverse cyberattack scenarios on the U.S. financial system. We use the Moody's Analytics Global Macroeconomic Model to trace the channels and economic consequences of each attack. The first scenario considers the economic fallout of a deposit run, precipitated by successive cyberattacks on small and medium-size financial institutions. The second scenario explores a cyberattack that paralyzes the retail payments system. Though differing in timing and magnitude, the economic damage in each scenario is meaningful.

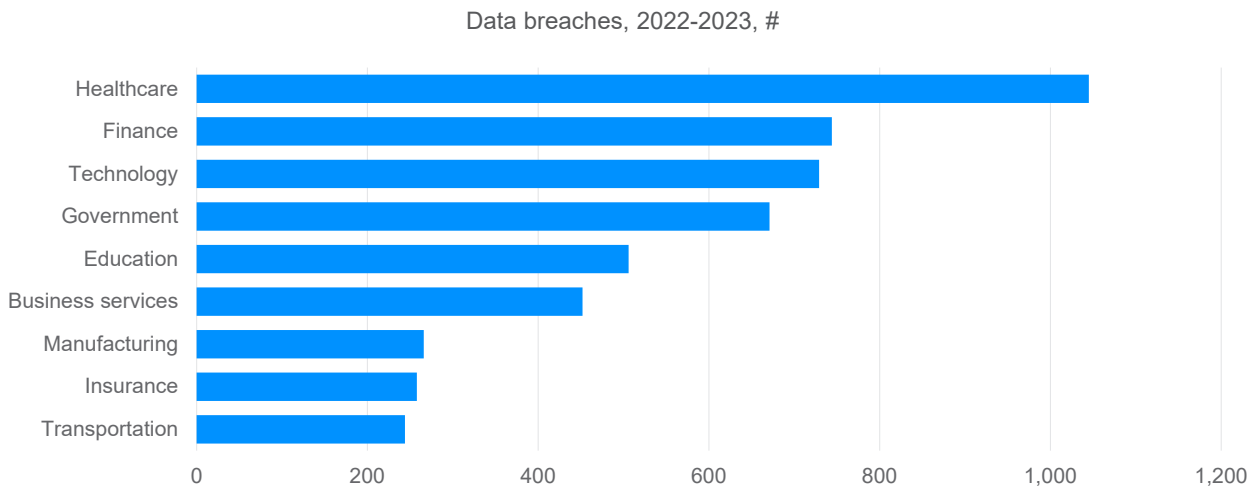
Seeds of contagion

Cyber threats to the financial system are growing in severity, with recent attacks exposing significant vulnerabilities. Financial institutions were subject to more successful cyberattacks than any other industry over the past two years except for healthcare (see Chart 1). The confidentiality of customer data, value of intellectual property, financial size, and reliance on third-party software providers make banks and financial institutions a primary target of cyber criminals.

While the frequency of cyberattacks has ebbed a bit in recent years, successful breaches have grown more damaging. Ransomware and other highly disruptive attacks have accounted for a higher share of breaches over the past six years (see Chart 2). Once the domain of more sophisticated cyber criminals or state-sponsored actors, ransomware attacks have proliferated with the rise of ransomware-as-a-service, enabling financially motivated cybercriminals to purchase or license malicious code to later deploy against potential targets.

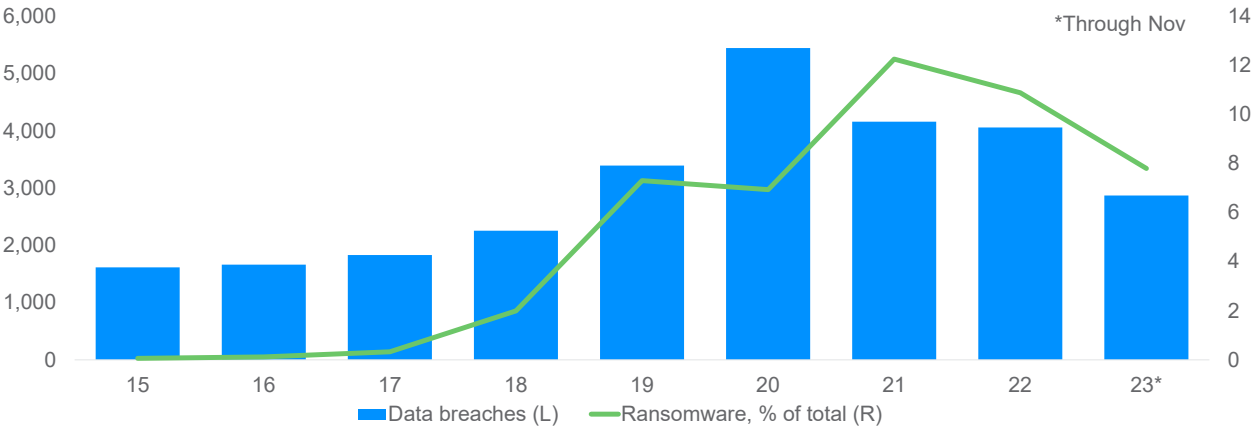
The rise of criminal ransomware gangs has coincided with a string of highly disruptive attacks on financial institutions that have threatened to upend markets and undermine trust in the financial system. The January 2023 ransomware breach of ION Trading Technologies—a Dublin-based derivatives trading platform operating in commodity markets—disrupted trading for more than a week by forcing market makers to

Chart 1: Finance, Tech, Healthcare in the Eye of the Storm



Sources: BitSight, Moody's Analytics

Chart 2: Fewer Breaches, Growing Severity

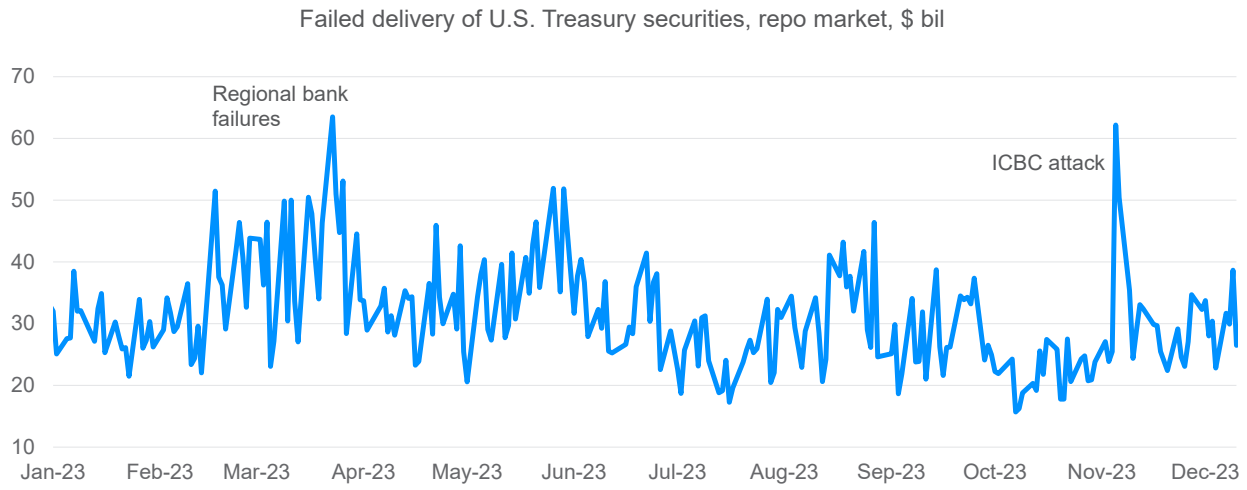


Sources: BitSight, Moody's Analytics

manually record trades. The hit to liquidity was amplified via counterparties' exposures and the loss of price-matching opportunities during the platform's outage.

More concerning still was the November ransomware attack on ICBC Financial Services, a U.S. subsidiary of the Industrial and Commercial Bank of China. ICBC provides securities trading and clearing services in the U.S. Treasury and repo markets. At the height of the attack, ICBC's internal IT teams were forced to unplug the firm's servers and sever connections to the rest of the financial system. The outages rapidly siphoned liquidity from the U.S. Treasury market and spurred the second-largest single-day failure of repo trades last year (see Chart 3).

Chart 3: Cyber Contagion a Real Concern



Sources: DTCC, Moody's Analytics

That ICBC is a relatively small player in both the Treasury and repo markets underscores the vulnerability of the financial system to attacks on seemingly isolated parts of the system. While damage to the broader financial system from the ION and ICBC attacks was ultimately contained, the possibility of a future attack with broader contagion effects is no longer a remote one. The severity of the breaches also points to the potential for rapidly cascading losses despite growing investments in cybersecurity as well as the growing role of IT teams in executive reporting lines and corporate leadership.

Cyberattack scenarios

The financial system faces many cyber threats. These may include, on the one hand, a cyberattack on a commercial bank, other bank or nonbank financial institutions, or a group of banks or financial institutions. It also includes an attack on critical financial system infrastructure such as the payments system or a securities exchange. We have constructed two adverse scenarios that encompass these broad threats.

The first scenario begins with successive ransomware attacks that paralyze small and midsize banks, triggering a wave of deposit flight that culminates in a full-blown banking panic. While bank customers are unable to withdraw deposits for the duration of the attack, we assume that they grow fearful of another incident and pull deposits after the attack is resolved and access to deposits is restored. As depositors flee small and midsize banks for the perceived safety of larger institutions, a banking and financial crisis unfolds.

This scenario is grounded in the gaps in cyber preparedness between the largest banks and financial institutions and their smaller peers. Compared with larger financial institutions, small and midsize banks are less likely to conduct advanced cyber defense practices such as red team testing or penetration tests on at least a biannual basis. Security requirements for third-party vendors may also vary in stringency[1] (see Chart 4).

The second scenario examines the impact of a cyberattack on critical financial system infrastructure. Specifically, we assume that a cyberattack knocks out the Automated Clearing House network for a period

1 The Federal Reserve further documents gaps in cyber preparedness among small and medium-size banks in its 2022 and 2023 annual reports to Congress on cybersecurity and the resilience of the financial system. https://www.federalreserve.gov/publications/financial-stability-report.htm

Chart 4: Large Banks Report More Advanced Cyber Defense Practices

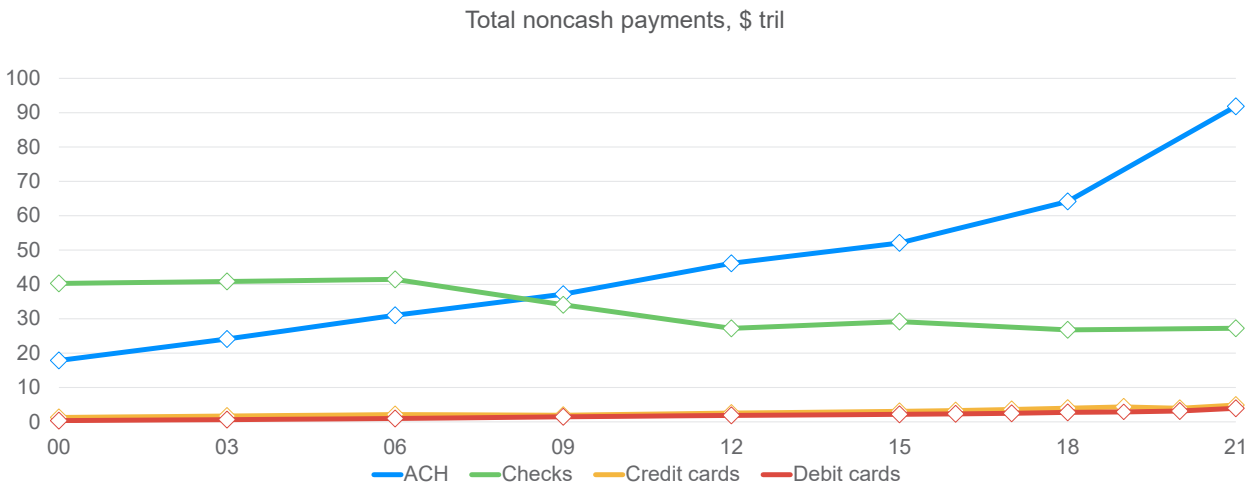
% of banks by assets

Cybersecurity practice	Frequency/scope	Large >$250 bil	Midsize $75-$250 bil	Small <$75 bil
Require multi-factor authentication for remote access to external resources	In all cases	87%	78%	71%
Require third-party vendors to give notice of cybersecurity incidences	In all cases	83%	56%	56%
Conduct penetration tests	At least twice yearly	78%	63%	63%
Conduct tabletop simulations	At least twice yearly	62%	54%	27%
Carry out red team/purple team testing	At least twice yearly	61%	38%	23%
Test incident response plans	Quarterly	29%	25%	9%
Back up data to resources that are disconnected from the bank's internal network	At least weekly	73%	100%	100%

Sources: MIS, BitSight, Moody's Analytics

of three weeks, paralyzing the retail payments system. There are rolling outages in the following month as operators work to restore full service. The ACH network is chosen for this scenario because of its role as the bedrock of the retail payments system, with transactions such as payroll direct deposit and electronic bill pay accounting for most noncash payments by dollar volume (see Chart 5). The ACH network is also the backbone of popular peer-to-peer payment services such as Venmo and PayPal.

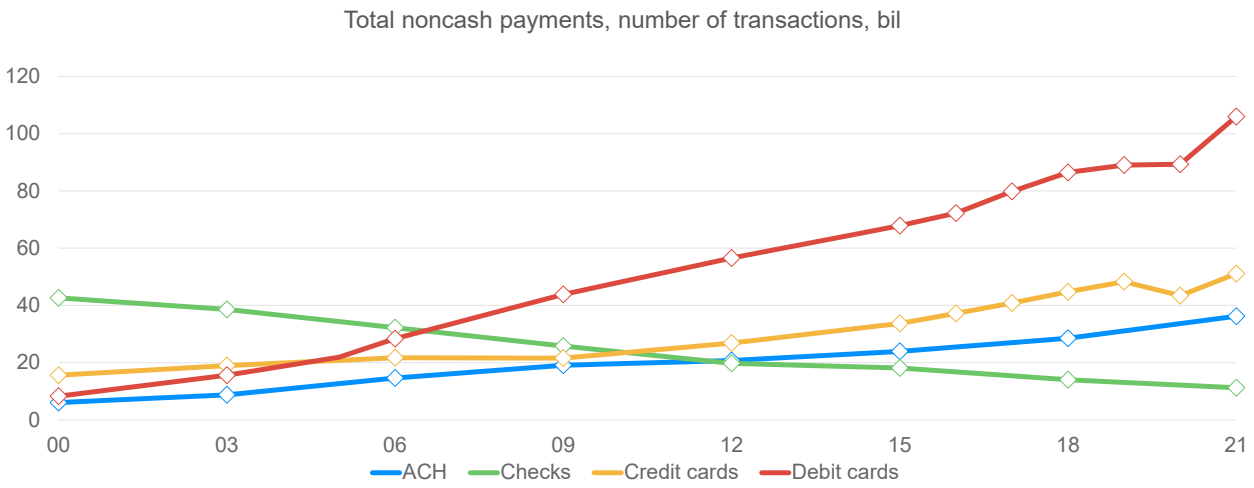
Chart 5: ACH the Bedrock of Retail Payments System



Sources: Federal Reserve, Moody's Analytics

While the ACH network accounts for most noncash payments by dollar volume, credit and debit cards are used more frequently in daily transactions (see Chart 6). We thus broaden our scenario assumptions to incorporate an interruption to credit card networks and payment services. In this dark scenario, credit card networks fear contagion and suspend service, forcing a mass migration from electronic payments to checks and cash.

Chart 6: Credit, Debit Cards Most Frequent Form of Payment



Sources: Federal Reserve, Moody's Analytics

Methodology

We use the Moody's Analytics Global Macroeconomic Model to examine the origins of the cyberattacks in each scenario and asses the economic consequences. The Moody's Analytics Global Macroeconomic Model is a large-scale structural model similar to those employed by the Federal Reserve and other global central banks. The model has been used to investigate a diverse set of economic policies and alternative scenarios, from the economic consequences of trade wars to the impact of pandemic-era fiscal policy and troubles in the commercial real estate market.

To create the first scenario, we translate scenario assumptions into specific shocks to bank lending standards, consumer confidence, stock market volatility, and corporate credit spreads. We use the behavior of banks and financial markets during historical periods of financial and banking stress to assist in the calibration of scenario shocks. The second scenario is constructed with specific shocks to consumer spending based on our assumption of a near-total blackout of the retail payments system. Additional shocks to consumer spending and financial market volatility are then layered on. A full list of key variables can be found in the appendix.

Cyber Deposit Run Scenario

In this scenario, successive ransomware attacks on small and medium-size banks paralyze banks' internal networks and lock depositors out of accounts. Each new breach inspires another wave of attacks, with successful breaches growing in frequency and severity. Though no single event has a large impact on business and consumer spending, the attacks are highly disruptive to consumer confidence. As the attacks unfold, depositors at affected institutions are unable to access bank statements and suffer interruptions to payment services for up to 10 business days.

The outages leave depositors unable to make or receive payments, transfer funds, or deposit or withdraw cash from bank branches or ATMs. While banks are ultimately able to restore service and ensure the integrity of customer data, concerns grow over the safety of deposits with each successive attack. As jitters intensify, banks that suffer greater reputational damage or larger interruptions of service begin to experi-

ence deposit outflows. Though unable to withdraw deposits for the duration of the attack, customers at the affected banks withdraw deposits once the attack is resolved and service is restored.

While slow at first, these withdrawals grow in velocity and number as more customers question the security of deposits after losing access during the cyberattacks. As the flight gathers steam, the panic spreads beyond the initial circle of compromised institutions. Fearing the security of their own deposits, customers at more small and medium-size banks flee, migrating to the perceived safety of larger institutions and money market funds. The dynamic is reminiscent of outflows experienced during the regional banking crisis in March, though on a larger scale (see Chart 7).

Chart 7: Regional Bank Failures Spur Deposit Flight

Sources: ICI, Moody's Analytics

In a bid to stem the flight, the Fed announces a program of liquidity injections for the hardest-hit banks, while regulators stand up a new facility to allow victims of cyberattacks to gain access to their deposits. However, the measures are unable to restore trust in the banking system and quell fears of further attacks on small and midsize institutions. As flight from small and medium-size banks intensifies, initial jitters metastasize into a full-blown banking panic, triggering the failure of dozens of small and midsize institutions and dragging the broader economy into recession.

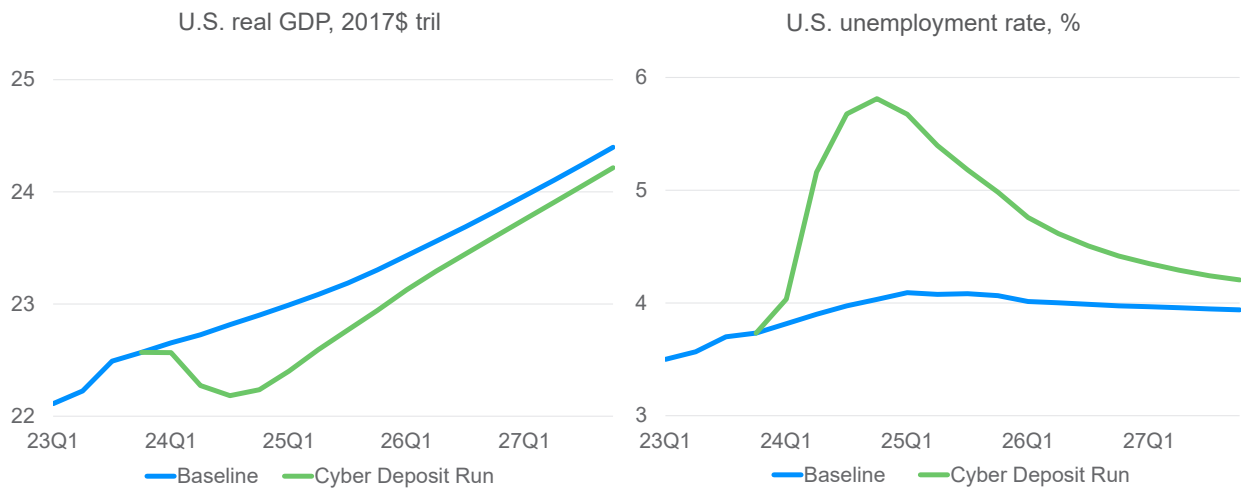
From recession to recovery

The flight from small and medium-size banks has a cascading effect, with initial bank failures triggering successive waves of deposit runs that push more small and midsize institutions to the edge. As the panic intensifies, financial markets seize up, with credit spreads and volatility spiking and interbank lending grinding to a halt. The run of bank failures causes financial market turmoil to intensify, triggering a broader stock market collapse. While the Fed slashes interest rates and provides emergency liquidity to stanch some of the bleeding, policymakers struggle to address a new breed of cyber-linked solvency fears. Many institutions fail and their assets sold to their larger peers.

As the panic intensifies, consumer and business spending plummets. Facing a spike in financing costs and uncertainty over the extent of the damage to the banking sector, businesses cut hours and slash payrolls,

precipitating a collapse in employment and incomes. Fearing job loss and a prolonged recession, households cut spending, furthering the cycle of job and income loss. After moving sideways, the economy falls into recession (see Chart 8 and Table 1).

Chart 8: Cyber Deposit Run Builds Slow, Burns Deep



Sources: BEA, BLS, Moody's Analytics

Though small and midsize banks are no less of a target for cyber criminals, hackers fall victim to their own success, with increased monitoring and investment in cyber defenses leading to a lull in new attacks. The small and midsize institutions able to survive the wave of bank failures take additional steps to bolster cyber resiliency, from bolstering investment in IT teams and network security to storing data in off-the-grid arrangements that allow for faster restoration of critical data and networks.

However, these changes take time to restore trust in the broader banking system. By the time larger banks are able to absorb failed institutions and remaining small and medium-size banks shore up cyber defenses, GDP falls some 1.7% peak to trough, with the unemployment rate spiking to nearly 6%. The shape of the ensuing recovery is slow given the deep scars inflicted on depositors, the damage to the banking system's DNA from the loss of critical client relationships, and the recession's lingering hit to consumer and business sentiment.

Payment System Collapse Scenario

In this second scenario, a ransomware attack on a large financial institution breaches the ACH network, encrypting critical files and bringing all ACH network traffic to a halt. As the self-replicating worm overwhelms the network's computers and servers, requests by banks to send and receive ACH payment files are denied. Though operators work to isolate the attack, the discovery of missing or compromised data forces the shutdown of more network assets, complicating early efforts to restore service.

Fearing that problems plaguing the ACH system will spread to credit card networks, major network operators preemptively suspend service, leaving cardholders unable to use cards for payments. The disruptions culminate in the near-complete paralysis of the retail payments system with banks, businesses and consumers unable to send or receive funds electronically. The attack also sidelines popular peer-to-peer payment services that use the ACH network as a backbone.

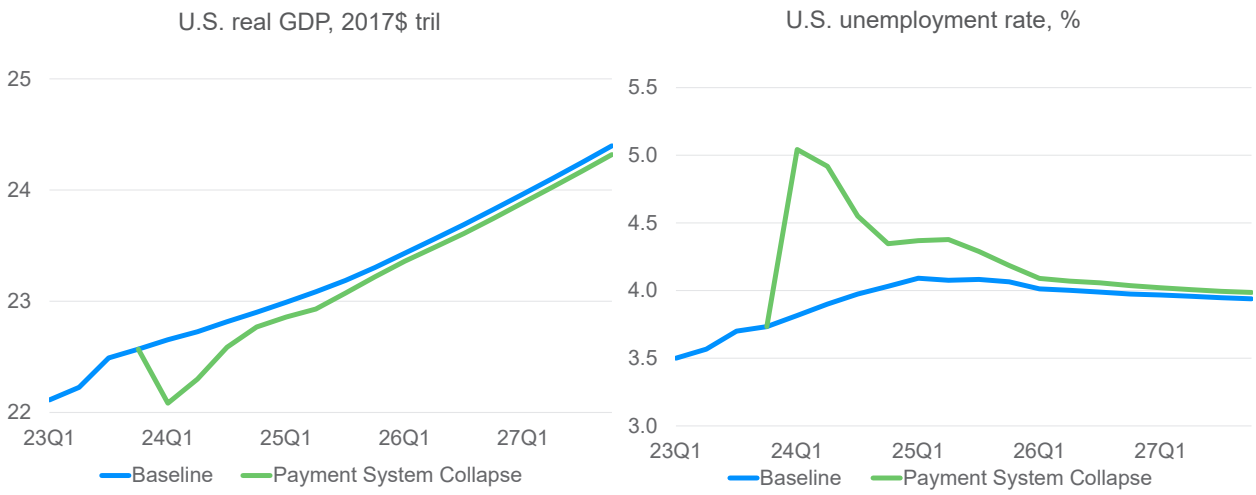
The initial damage forces the ACH network offline for a period of three weeks. Credit card networks are quicker to restore service as contagion fears subside. Though ACH operators are able to contain the initial attack and reconcile missing data, there are intermittent outages in the subsequent four weeks as network operators struggle to bring the full system back online.

News of the ACH attack spreads slowly at first, with bank and card customers still able to log into bank accounts and review bank and credit card statements. However, fears escalate as common ACH transactions such as payroll direct deposit and electronic bill payments fail to post. The blow to consumers' psyches grows more tangible as credit card payments are rejected or denied.

With paychecks in limbo and concerns over overdue bills and credit card fees mounting, consumers sharply curtail spending and restrict purchases to essential goods. Forced to abandon credit cards for cash and checks, checkout lines at supermarkets, retail stores and gas stations swell, stirring panic of a permanent collapse in the electronic payments system. Small businesses run into their own troubles, with reduced consumer spending limiting revenues and forcing them to renegotiate payments to suppliers.

In a bid to restore confidence, the government announces a short-term forbearance program for consumer and business loans. Employers are encouraged to distribute paychecks in person or by mail. However, spending nosedives amid the breakdown in the payments system and households' fear of a more permanent disruption, precipitating a near-vertical drop in economic activity. Spending boomerangs once the ACH network is fully repaired, with pent-up demand for goods and services rapidly returning the economy to growth. However, the blow to sentiment from the collapse in electronic payments lingers, and output takes more than a quarter to surpass its previous peak (see Chart 9).

Chart 9: Abrupt Decline, Delayed Recovery



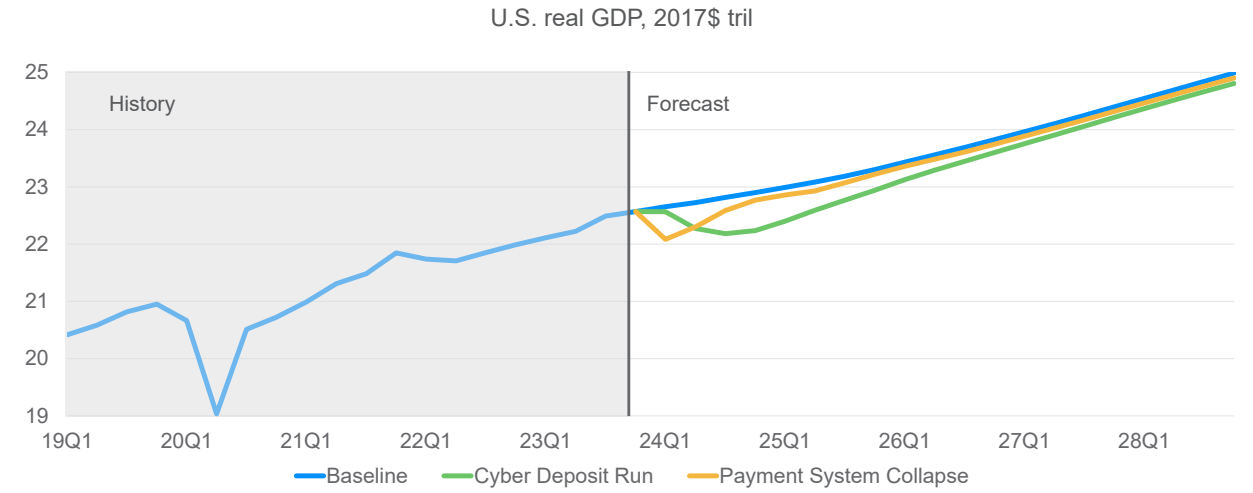
Sources: BEA, BLS, Moody's Analytics

Sharp drop, incomplete recovery

The economic damage wrought by the ACH attack takes a different course than the series of cyber incidents at small and medium-size banks (see Charts 10 and 11). Output in this scenario drops immediately as the

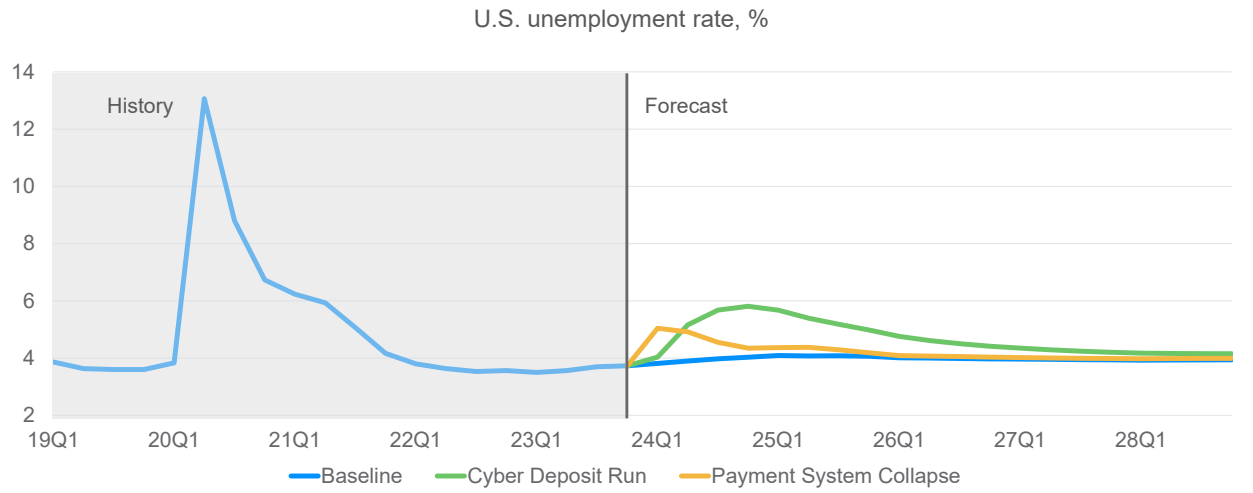
knockout of the ACH network leaves households out of a paycheck and the freezing of credit card networks limits consumer payments to personal checks and cash. Smaller businesses face growing demands to pay workers in cash, deepening the crunch and forcing some businesses to curtail hours and operations. While the immediate impact is a decline in business consumption spending, business investment slumps as sentiment darkens.

Chart 10: Comparing the Two Cyber Scenarios



Sources: BEA, Moody's Analytics

Chart 11: Comparing the Two Cyber Scenarios



Sources: BEA, Moody's Analytics

Though the ACH network is eventually restored, the near seven-week interruption of payment services initially sends shock waves through financial markets. Disruptions in credit markets are initially severe, with credit spreads spiking and banks pulling back on lending. However, the damage falls short of a financial crisis. Despite the reversion to checks and cash, the financial system continues to perform

core functions of credit allocation. Helping matters is that the digital infrastructure underpinning securities markets is not impaired.

An emergency rate cut by the Fed cements faith among financial market participants that the blow to the retail payments system will prove temporary and that Fed officials stand ready to stave off a broader crisis. To prevent a wave of defaults, legislators enact rapid relief for banks, businesses and consumers, enabling banks to waive overdraft and late fees and provide a cushion for overdue bills.

That the financial system avoids a full meltdown does not mean the ensuing contraction is not painful. The initial drop in output in this scenario is greater than in the first scenario given frictions imposed on business and consumer spending and fears of a permanent loss of access to incomes and savings. Though financial market turmoil eases, the increase in precautionary savings by consumers and businesses transforms what is initially a cyber-induced supply shock into a full-fledged downturn. While the recovery is ultimately more rapid than the first scenario, the lingering blow to consumer sentiment prevents output from recovering more quickly.

A not-so-brave new world

Banks and other financial institutions are dedicating an increasing share of their investment to protecting proprietary and customer data.[2] Efforts to mitigate cyber threats will also play a growing role in the regulatory landscape. This year, the European Central Bank will conduct stress tests of supervised banks involving a simulated cyberattack that disrupts banks' daily operations, marking the broadest mandatory assessment by a major bank regulator to date.[3] Supervised institutions will be evaluated on their ability to overcome the initial attack and length of time in restoring normal business operations. The test was announced last year amid growing concerns over cyberattacks launched by nation states and state-affiliated adversaries.

This paper assesses the interaction between cyber-compromised institutions and the broader economy under a more general set of cyberattack assumptions. So far, the financial sector has been largely successful in heading off a massive cyber event. However, recent cyberattacks have exposed new vulnerabilities in the financial sector's increasingly interlinked plumbing. They also reveal the speed at which an attack on a seemingly isolated node can have systemic consequences.

The potential for a cyber-induced deposit run takes on new relevance in the wake of the failure of Silicon Valley Bank and the ensuing banking panic in March. The predominance of mobile banking apps and the ability to transfer funds at the stroke of a finger make a cyber-inspired banking panic a very real threat and one that could be especially damaging. We do not explicitly model an attack on a major securities exchange or third-party financial or IT services provider in this paper. However, a successful cyberattack on critical financial system infrastructure could follow a course of events like those outlined in the second scenario.

2 According to a Moody's Investors Service survey of more than 370 global financial institutions, spending on cybersecurity as a share of financial institutions' overall technology budgets has risen more than 50% in the past four years. See "Cyber budgets increase, executive overview improves, but challenges lurk under the surface", Sep 2023

3 See ECB to stress-test banks' ability to recover from cyberattack, Jan 3, 2024

The two scenarios explored in this paper involve assumptions regarding threat actors and the response of financial institutions and consumers that will surely vary in a real-world attack. However, given the heightened uncertainty and incomplete information likely to characterize a large-scale cyberattack, we assume missteps by depositors, financial institutions, and financial system regulators. In each scenario, animal spirits play a central role. Cyber defense practices would do well to anticipate them.

Table 1: Economic Impact of Cyberattack Scenarios

	24Q1	24Q2	24Q3	24Q4	25Q1	25Q2	25Q3	25Q4	26Q1	26Q2	26Q3	26Q4	2024	2025	2026	2027	2028
Gross domestic product, annualized % change																	
Baseline	1.5	1.3	1.6	1.5	1.6	1.6	1.8	2.0	2.2	2.2	2.2	2.3	1.9	1.6	2.1	2.3	2.4
Cyber Deposit Run	-0.0	-5.1	-1.6	1.0	3.0	3.5	3.1	3.1	3.3	2.9	2.7	2.7	-0.2	1.6	3.0	2.6	2.5
Difference from baseline	*-1.6*	*-6.4*	*-3.2*	*-0.5*	*1.4*	*1.8*	*1.4*	*1.0*	*1.1*	*0.7*	*0.5*	*0.3*	*-2.1*	*0.0*	*1.0*	*0.3*	*0.1*
Payment System Collapse	-8.3	4.0	5.2	3.3	1.6	1.3	2.5	2.6	2.4	2.1	2.1	2.3	0.4	2.6	2.3	2.3	2.4
Difference from baseline	*-9.9*	*2.7*	*3.6*	*1.8*	*-0.0*	*-0.4*	*0.7*	*0.6*	*0.2*	*-0.1*	*-0.1*	*0.0*	*-1.5*	*1.0*	*0.2*	*0.0*	*-0.0*
Gross domestic product, 2017$ tril																	
Baseline	22.7	22.7	22.8	22.9	23.0	23.1	23.2	23.3	23.4	23.6	23.7	23.8	22.8	23.1	23.6	24.2	24.8
Cyber Deposit Run	22.6	22.3	22.2	22.2	22.4	22.6	22.8	22.9	23.1	23.3	23.4	23.6	22.3	22.7	23.4	24.0	24.6
% difference from baseline	*-0.4*	*-2.0*	*-2.8*	*-2.9*	*-2.6*	*-2.1*	*-1.8*	*-1.6*	*-1.3*	*-1.1*	*-1.0*	*-0.9*	*-2.0*	*-2.0*	*-1.1*	*-0.8*	*-0.7*
Payment System Collapse	22.1	22.3	22.6	22.8	22.9	22.9	23.1	23.2	23.4	23.5	23.6	23.7	22.4	23.0	23.5	24.1	24.7
% difference from baseline	*-2.5*	*-1.9*	*-1.0*	*-0.6*	*-0.6*	*-0.7*	*-0.5*	*-0.4*	*-0.3*	*-0.3*	*-0.3*	*-0.3*	*-1.5*	*-0.5*	*-0.3*	*-0.3*	*-0.3*
Unemployment rate, %																	
Baseline	3.8	3.9	4.0	4.0	4.1	4.1	4.1	4.1	4.0	4.0	4.0	4.0	3.9	4.1	4.0	4.0	3.9
Cyber Deposit Run	4.0	5.2	5.7	5.8	5.7	5.4	5.2	5.0	4.8	4.6	4.5	4.4	5.2	5.3	4.6	4.3	4.2
Difference from baseline	*0.2*	*1.3*	*1.7*	*1.8*	*1.6*	*1.3*	*1.1*	*0.9*	*0.7*	*0.6*	*0.5*	*0.4*	*1.2*	*1.2*	*0.6*	*0.3*	*0.2*
Payment System Collapse	5.0	4.9	4.6	4.3	4.4	4.4	4.3	4.2	4.1	4.1	4.1	4.0	4.7	4.3	4.1	4.0	4.0
Difference from baseline	*1.2*	*1.0*	*0.6*	*0.3*	*0.3*	*0.3*	*0.2*	*0.1*	*0.1*	*0.1*	*0.1*	*0.1*	*0.8*	*0.2*	*0.1*	*0.0*	*0.1*
Nonfarm employment, mil																	
Baseline	157.4	157.6	157.8	158.0	158.1	158.3	158.5	158.6	158.7	158.9	159.0	159.1	157.7	158.4	158.9	159.4	160.0
Cyber Deposit Run	157.0	155.6	154.5	154.1	154.4	155.0	155.5	156.0	156.4	156.8	157.1	157.4	155.3	155.2	156.9	158.0	158.8
Difference from baseline	*-0.4*	*-2.0*	*-3.4*	*-3.8*	*-3.7*	*-3.3*	*-2.9*	*-2.6*	*-2.3*	*-2.1*	*-1.9*	*-1.7*	*-2.4*	*-3.1*	*-2.0*	*-1.4*	*-1.1*
Payment System Collapse	154.9	155.2	156.2	156.9	157.2	157.3	157.6	157.9	158.1	158.3	158.4	158.6	155.8	157.5	158.4	158.9	159.5
Difference from baseline	*-2.5*	*-2.4*	*-1.6*	*-1.1*	*-1.0*	*-1.0*	*-0.9*	*-0.7*	*-0.6*	*-0.6*	*-0.6*	*-0.5*	*-1.9*	*-0.9*	*-0.6*	*-0.5*	*-0.4*
S&P 500, 1941-43=10, NSA																	
Baseline	4,488.5	4,606.1	4,657.5	4,672.7	4,687.0	4,712.1	4,743.6	4,796.2	4,849.2	4,906.6	4,971.5	5,043.2	4,606.2	4,734.7	4,942.6	5,249.1	5,554.8
Cyber Deposit Run	3,927.2	3,816.6	3,794.1	3,813.4	3,865.0	3,943.3	4,029.5	4,131.2	4,231.0	4,330.0	4,430.4	4,533.5	3,837.8	3,992.2	4,381.2	4,804.5	5,188.8
% difference from baseline	*-12.5*	*-17.1*	*-18.5*	*-18.4*	*-17.5*	*-16.3*	*-15.1*	*-13.9*	*-12.7*	*-11.8*	*-10.9*	*-10.1*	*-16.7*	*-15.7*	*-11.4*	*-8.5*	*-6.6*
Payment System Collapse	4,155.4	4,184.7	4,252.8	4,301.8	4,337.3	4,375.7	4,428.7	4,501.9	4,570.5	4,639.3	4,713.4	4,794.5	4,223.7	4,410.9	4,679.4	5,022.0	5,356.1
% difference from baseline	*-7.4*	*-9.1*	*-8.7*	*-7.9*	*-7.5*	*-7.1*	*-6.6*	*-6.1*	*-5.7*	*-5.4*	*-5.2*	*-4.9*	*-8.3*	*-6.8*	*-5.3*	*-4.3*	*-3.6*
Fed funds rate, %																	
Baseline	5.3	5.1	4.7	4.5	4.3	4.1	3.8	3.8	3.5	3.3	3.0	3.0	4.9	4.0	3.2	2.9	2.8
Cyber Deposit Run	5.2	4.3	3.1	2.8	2.6	2.4	2.2	2.3	2.1	2.0	1.8	1.8	3.9	2.4	1.9	2.1	2.3
Difference from baseline	*-0.10*	*-0.83*	*-1.57*	*-1.74*	*-1.72*	*-1.65*	*-1.57*	*-1.49*	*-1.42*	*-1.34*	*-1.24*	*-1.13*	*-1.06*	*-1.61*	*-1.28*	*-0.84*	*-0.47*
Payment System Collapse	5.0	4.6	4.1	4.0	3.8	3.6	3.3	3.4	3.2	3.0	2.7	2.7	4.4	3.5	2.9	2.8	2.7
Difference from baseline	*-0.29*	*-0.50*	*-0.54*	*-0.53*	*-0.50*	*-0.48*	*-0.45*	*-0.39*	*-0.34*	*-0.30*	*-0.26*	*-0.23*	*-0.46*	*-0.45*	*-0.28*	*-0.15*	*-0.06*
U.S. 10-yr Treasury yield																	
Baseline	4.2	4.2	4.1	4.1	4.1	4.1	4.0	4.0	4.0	4.0	4.0	4.0	4.2	4.1	4.0	4.0	4.0
Cyber Deposit Run	4.2	3.8	3.5	3.4	3.4	3.4	3.4	3.4	3.5	3.5	3.5	3.5	3.7	3.4	3.5	3.7	3.8
Difference from baseline	*-0.04*	*-0.37*	*-0.61*	*-0.69*	*-0.70*	*-0.67*	*-0.64*	*-0.61*	*-0.58*	*-0.55*	*-0.51*	*-0.47*	*-0.43*	*-0.66*	*-0.53*	*-0.35*	*-0.17*
Payment System Collapse	4.1	4.0	3.9	3.9	3.9	3.9	3.8	3.8	3.9	3.9	3.9	3.9	4.0	3.9	3.9	3.9	4.0
Difference from baseline	*-0.11*	*-0.20*	*-0.22*	*-0.22*	*-0.21*	*-0.21*	*-0.20*	*-0.19*	*-0.17*	*-0.16*	*-0.15*	*-0.14*	*-0.19*	*-0.21*	*-0.15*	*-0.10*	*-0.05*

Sources: BSA, BLS, S&P, and Moody's Analytics

Appendix: Key Model Variables for Cyberattack Scenarios

The Moody's Analytics Global Macroeconomic Model can be used to evaluate a broad range of economic policies and produce forecasts under a set of baseline and alternative assumptions. The cyberattack scenarios explored in this paper were created by translating scenario-specific assumptions into exogenous adjustments to key variables in the model. These variables describe the behavior of banks, financial market participants, businesses, and consumers. The following list summarizes the variables used to create each scenario and the reasoning behind each adjustment.

Variable	Moody's Analytics Mnemonic	Rationale for adjustment
S&P 500 Volatility	FSPVOL.IUSA	The Standard & Poor's historical volatility index is the primary lever in the model for capturing short-term financial market strain. Adjustments to the index flow through to equity prices, interest rates, credit risk spreads, and liquidity. We shock the index in both the Cyber Deposit Run and Payment System Collapse scenarios to reflect the two scenarios' differing degrees of financial strain.
Net % of banks tightening standards for credit card loans	FXSLASINCCQ.IUSA	Periods of intense strain in financial markets are marked by not only higher financing costs but also a decline in short-term liquidity and lenders' willingness to extend credit. These four variables from the Federal Reserve Senior Loan Officer Survey are incorporated in the model as a proxy for short-term liquidity as well as lending to the real economy. We shock these four variables in the Cyber Deposit Run scenario to capture the dynamics of an acute and deepening financial crisis and its effects on the broader economy.
Net % of banks tightening standards for mortgage loans	FXSLASHMQ.IUSA	
Net % of banks tightening standards for CRE loans	FXSLASREQ.IUSA	
Net % of banks tightening standards for C&I loans	FXSLASCILQ.IUSA	
Consumer Confidence Index	FCBC.IUSA	The Conference Board's Consumer Confidence Index is the primary measure of consumer sentiment in the model and has broad linkages throughout. Adjustments to the consumer confidence index flow through to consumer spending, employment, labor force participation, inflation expectations, and business sentiment as well as financial market volatility. In the Cyber Deposit Run scenario, we shock consumer confidence to capture the dynamics of a bank run, cementing the link between the strain on liquidity and consumers' spending and saving decisions. In the Payment System Collapse scenario, we shock consumer confidence to amplify the impact of the payment system outage on consumer spending and sentiment.
S&P 500 Crash Indicator	FDUMSP500Q.IUSA	The S&P 500 Crash Indicator is a dummy variable activated in each scenario to amplify the transmission mechanism between financial market strain and equity price declines.
Personal consumption expenditures—durable goods ex motor vehicles	FCDXMVP$.IUSA	In the Payment System Collapse scenario, we directly shock consumer goods and services spending to reflect assumptions regarding the share of forgone spending during the initial crash of the ACH network and suspension of credit card payments. After inputting the initial consumption shocks during the first quarter of the forecast, we allow the model to solve each component of consumption endogenously over the rest of the forecast horizon.
Personal consumption expenditures—motor vehicles and parts	FCDMVP$.IUSA	
Personal consumption expenditures—nondurable goods	FCN$.IUSA	
Personal consumption expenditures—services	FCS$.IUSA	

Source: Moody's Analytics

About the Authors

Jesse Rogers is an assistant director and economist at Moody's Analytics, covering Latin America and Emerging Asia. His research spans trade policy, international capital flows, commodity markets, and economic development. Jesse holds a master's degree in economics and international relations from the Johns Hopkins School of Advanced International Studies. While completing his degree, he interned with the U.S. Treasury and Institute of International Finance. Previously, he was a finance and politics reporter for El Diario New York and worked in Mexico City for the Center for Research and Teaching in Economics (CIDE). He received his bachelor's degree in Hispanic studies at the University of Pennsylvania.

Matt Colyar is an economist at Moody's Analytics in King of Prussia PA. His work is primarily focused on the labor market and monetary policy in the U.S. He also covers the economies of Pennsylvania, Missouri, and several U.S. metro areas. Prior to joining Moody's Analytics, Matt worked at the World Bank, focusing on private-sector development in South Asian countries, and in private industry as a financial analyst. He received his master's degree in applied economics from Lehigh University and his bachelor's degree in business administration from West Chester University.

Mark Zandi is chief economist of Moody's Analytics, where he directs economic research. Moody's Analytics, a subsidiary of Moody's Corp., is a leading provider of economic research, data and analytical tools. Dr. Zandi is a cofounder of Economy.com, which Moody's purchased in 2005.

Dr. Zandi is on the board of directors of MGIC, the nation's largest private mortgage insurance company, and is the lead director of PolicyMap, a data visualization and analytics company, used by policymakers and commercial businesses.

He is a trusted adviser to policymakers and an influential source of economic analysis for businesses, journalists and the public. Dr. Zandi frequently testifies before Congress and conducts regular briefings on the economy for corporate boards, trade associations, and policymakers at all levels.

Dr. Zandi is the author of Paying the Price: Ending the Great Recession and Beginning a New American Century, which provides an assessment of the monetary and fiscal policy response to the Great Recession. His other book, Financial Shock: A 360º Look at the Subprime Mortgage Implosion, and How to Avoid the Next Financial Crisis, is described by The New York Times as the "clearest guide" to the financial crisis. Dr. Zandi is host of the Inside Economics podcast.

Dr. Zandi earned his BS from the Wharton School at the University of Pennsylvania and his PhD at the University of Pennsylvania.

About Moody's Analytics

Moody's Analytics provides financial intelligence and analytical tools supporting our clients' growth, efficiency and risk management objectives. The combination of our unparalleled expertise in risk, expansive information resources, and innovative application of technology helps today's business leaders confidently navigate an evolving marketplace. We are recognized for our industry-leading solutions, comprising research, data, software and professional services, assembled to deliver a seamless customer experience. Thousands of organizations worldwide have made us their trusted partner because of our uncompromising commitment to quality, client service, and integrity.

Concise and timely economic research by Moody's Analytics supports firms and policymakers in strategic planning, product and sales forecasting, credit risk and sensitivity management, and investment research. Our economic research publications provide in-depth analysis of the global economy, including the U.S. and all of its state and metropolitan areas, all European countries and their subnational areas, Asia, and the Americas. We track and forecast economic growth and cover specialized topics such as labor markets, housing, consumer spending and credit, output and income, mortgage activity, demographics, central bank behavior, and prices. We also provide real-time monitoring of macroeconomic indicators and analysis on timely topics such as monetary policy and sovereign risk. Our clients include multinational corporations, governments at all levels, central banks, financial regulators, retailers, mutual funds, financial institutions, utilities, residential and commercial real estate firms, insurance companies, and professional investors.

Moody's Analytics added the economic forecasting firm Economy.com to its portfolio in 2005. This unit is based in King of Prussia PA, a suburb of Philadelphia, with offices in London, Prague and Sydney. More information is available at www.economy.com.

Moody's Analytics is a subsidiary of Moody's Corporation (NYSE: MCO). Further information is available at www.moodysanalytics.com.

About Moody's Corporation

Moody's Analytics is a subsidiary of Moody's Corporation (NYSE: MCO). MCO reported revenue of $5.5 billion in 2022, employs approximately 14,000 people worldwide and maintains a presence in more than 40 countries. Further information about Moody's Analytics is available at www.moodysanalytics.com.

CREDIT RATINGS ISSUED BY MOODY'S CREDIT RATINGS AFFILIATES ARE THEIR CURRENT OPINIONS OF THE RELATIVE FUTURE CREDIT RISK OF ENTITIES, CREDIT COMMITMENTS, OR DEBT OR DEBT-LIKE SECURITIES, AND MATERIALS, PRODUCTS, SERVICES AND INFORMATION PUBLISHED OR OTHERWISE MADE AVAILABLE BY MOODY'S (COLLECTIVELY, "MATERIALS") MAY INCLUDE SUCH CURRENT OPINIONS. MOODY'S DEFINES CREDIT RISK AS THE RISK THAT AN ENTITY MAY NOT MEET ITS CONTRACTUAL FINANCIAL OBLIGATIONS AS THEY COME DUE AND ANY ESTIMATED FINANCIAL LOSS IN THE EVENT OF DEFAULT OR IMPAIRMENT. SEE APPLICABLE MOODY'S RATING SYMBOLS AND DEFINITIONS PUBLICATION FOR INFORMATION ON THE TYPES OF CONTRACTUAL FINANCIAL OBLIGATIONS ADDRESSED BY MOODY'S CREDIT RATINGS. CREDIT RATINGS DO NOT ADDRESS ANY OTHER RISK, INCLUDING BUT NOT LIMITED TO: LIQUIDITY RISK, MARKET VALUE RISK, OR PRICE VOLATILITY. CREDIT RATINGS, NON-CREDIT ASSESSMENTS ("ASSESSMENTS"), AND OTHER OPINIONS INCLUDED IN MOODY'S MATERIALS ARE NOT STATEMENTS OF CURRENT OR HISTORICAL FACT. MOODY'S MATERIALS MAY ALSO INCLUDE QUANTITATIVE MODEL-BASED ESTIMATES OF CREDIT RISK AND RELATED OPINIONS OR COMMENTARY PUBLISHED BY MOODY'S ANALYTICS, INC. AND/OR ITS AFFILIATES. MOODY'S CREDIT RATINGS, ASSESSMENTS, OTHER OPINIONS AND MATERIALS DO NOT CONSTITUTE OR PROVIDE INVESTMENT OR FINANCIAL ADVICE, AND MOODY'S CREDIT RATINGS, ASSESSMENTS, OTHER OPINIONS AND MATERIALS ARE NOT AND DO NOT PROVIDE RECOMMENDATIONS TO PURCHASE, SELL, OR HOLD PARTICULAR SECURITIES. MOODY'S CREDIT RATINGS, ASSESSMENTS, OTHER OPINIONS AND MATERIALS DO NOT COMMENT ON THE SUITABILITY OF AN INVESTMENT FOR ANY PARTICULAR INVESTOR. MOODY'S ISSUES ITS CREDIT RATINGS, ASSESSMENTS AND OTHER OPINIONS AND PUBLISHES OR OTHERWISE MAKES AVAILABLE ITS MATERIALS WITH THE EXPECTATION AND UNDERSTANDING THAT EACH INVESTOR WILL, WITH DUE CARE, MAKE ITS OWN STUDY AND EVALUATION OF EACH SECURITY THAT IS UNDER CONSIDERATION FOR PURCHASE, HOLDING, OR SALE.

MOODY'S CREDIT RATINGS, ASSESSMENTS, OTHER OPINIONS, AND MATERIALS ARE NOT INTENDED FOR USE BY RETAIL INVESTORS AND IT WOULD BE RECKLESS AND INAPPROPRIATE FOR RETAIL INVESTORS TO USE MOODY'S CREDIT RATINGS, ASSESSMENTS, OTHER OPINIONS OR MATERIALS WHEN MAKING AN INVESTMENT DECISION. IF IN DOUBT YOU SHOULD CONTACT YOUR FINANCIAL OR OTHER PROFESSIONAL ADVISER.

ALL INFORMATION CONTAINED HEREIN IS PROTECTED BY LAW, INCLUDING BUT NOT LIMITED TO, COPYRIGHT LAW, AND NONE OF SUCH INFORMATION MAY BE COPIED OR OTHERWISE REPRODUCED, REPACKAGED, FURTHER TRANSMITTED, TRANSFERRED, DISSEMINATED, REDISTRIBUTED OR RESOLD, OR STORED FOR SUBSEQUENT USE FOR ANY SUCH PURPOSE, IN WHOLE OR IN PART, IN ANY FORM OR MANNER OR BY ANY MEANS WHATSOEVER, BY ANY PERSON WITHOUT MOODY'S PRIOR WRITTEN CONSENT. FOR CLARITY, NO INFORMATION CONTAINED HEREIN MAY BE USED TO DEVELOP, IMPROVE, TRAIN OR RETRAIN ANY SOFTWARE PROGRAM OR DATABASE, INCLUDING, BUT NOT LIMITED TO, FOR ANY ARTIFICIAL INTELLIGENCE, MACHINE LEARNING OR NATURAL LANGUAGE PROCESSING SOFTWARE, ALGORITHM, METHODOLOGY AND/OR MODEL.

MOODY'S CREDIT RATINGS, ASSESSMENTS, OTHER OPINIONS AND MATERIALS ARE NOT INTENDED FOR USE BY ANY PERSON AS A BENCHMARK AS THAT TERM IS DEFINED FOR REGULATORY PURPOSES AND MUST NOT BE USED IN ANY WAY THAT COULD RESULT IN THEM BEING CONSIDERED A BENCHMARK.

All information contained herein is obtained by MOODY'S from sources believed by it to be accurate and reliable. Because of the possibility of human or mechanical error as well as other factors, however, all information contained herein is provided "AS IS" without warranty of any kind. MOODY'S adopts all necessary measures so that the information it uses in assigning a credit rating is of sufficient quality and from sources MOODY'S considers to be reliable including, when appropriate, independent third-party sources. However, MOODY'S is not an auditor and cannot in every instance independently verify or validate information received in the credit rating process or in preparing its Materials.

To the extent permitted by law, MOODY'S and its directors, officers, employees, agents, representatives, licensors and suppliers disclaim liability to any person or entity for any indirect, special, consequential, or incidental losses or damages whatsoever arising from or in connection with the information contained herein or the use of or inability to use any such information, even if MOODY'S or any of its directors, officers, employees, agents, representatives, licensors or suppliers is advised in advance of the possibility of such losses or damages, including but not limited to: (a) any loss of present or prospective profits or (b) any loss or damage arising where the relevant financial instrument is not the subject of a particular credit rating assigned by MOODY'S.

To the extent permitted by law, MOODY'S and its directors, officers, employees, agents, representatives, licensors and suppliers disclaim liability for any direct or compensatory losses or damages caused to any person or entity, including but not limited to by any negligence (but excluding fraud, willful misconduct or any other type of liability that, for the avoidance of doubt, by law cannot be excluded) on the part of, or any contingency within or beyond the control of, MOODY'S or any of its directors, officers, employees, agents, representatives, licensors or suppliers, arising from or in connection with the information contained herein or the use of or inability to use any such information.

NO WARRANTY, EXPRESS OR IMPLIED, AS TO THE ACCURACY, TIMELINESS, COMPLETENESS, MERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE OF ANY CREDIT RATING, ASSESSMENT, OTHER OPINION OR INFORMATION IS GIVEN OR MADE BY MOODY'S IN ANY FORM OR MANNER WHATSOEVER.

Moody's Investors Service, Inc., a wholly-owned credit rating agency subsidiary of Moody's Corporation ("MCO"), hereby discloses that most issuers of debt securities (including corporate and municipal bonds, debentures, notes and commercial paper) and preferred stock rated by Moody's Investors Service, Inc. have, prior to assignment of any credit rating, agreed to pay to Moody's Investors Service, Inc. for credit ratings opinions and services rendered by it fees ranging from $500 to approximately $5,300,000. MCO and Moody's Investors Service also maintain policies and procedures to address the independence of Moody's Investors Service credit ratings and credit rating processes. Information regarding certain affiliations that may exist between directors of MCO and rated entities, and between entities who hold credit ratings from Moody's Investors Service, Inc. and have also publicly reported to the SEC an ownership interest in MCO of more than 5%, is posted annually at www.moodys.com under the heading "Investor Relations — Corporate Governance — Charter Documents - Director and Shareholder Affiliation Policy."

Moody's SF Japan K.K., Moody's Local AR Agente de Calificación de Riesgo S.A., Moody's Local BR Agência de Classificação de Risco LTDA, Moody's Local MX S.A. de C.V, I.C.V., Moody's Local PE Clasificadora de Riesgo S.A., and Moody's Local PA Calificadora de Riesgo S.A. (collectively, the "Moody's Non-NRSRO CRAs") are all indirectly wholly-owned credit rating agency subsidiaries of MCO. None of the Moody's Non-NRSRO CRAs is a Nationally Recognized Statistical Rating Organization.

Additional terms for Australia only: Any publication into Australia of this document is pursuant to the Australian Financial Services License of MOODY'S affiliate, Moody's Investors Service Pty Limited ABN 61 003 399 657AFSL 336969 and/or Moody's Analytics Australia Pty Ltd ABN 94 105 136 972 AFSL 383569 (as applicable). This document is intended to be provided only to "wholesale clients" within the meaning of section 761G of the Corporations Act 2001. By continuing to access this document from within Australia, you represent to MOODY'S that you are, or are accessing the document as a representative of, a "wholesale client" and that neither you nor the entity you represent will directly or indirectly disseminate this document or its contents to "retail clients" within the meaning of section 761G of the Corporations Act 2001. MOODY'S credit rating is an opinion as to the creditworthiness of a debt obligation of the issuer, not on the equity securities of the issuer or any form of security that is available to retail investors.

Additional terms for India only: Moody's credit ratings, Assessments, other opinions and Materials are not intended to be and shall not be relied upon or used by any users located in India in relation to securities listed or proposed to be listed on Indian stock exchanges.

Additional terms with respect to Second Party Opinions (as defined in Moody's Investors Service Rating Symbols and Definitions): Please note that a Second Party Opinion ("SPO") is not a "credit rating". The issuance of SPOs is not a regulated activity in many jurisdictions, including Singapore. JAPAN: In Japan, development and provision of SPOs fall under the category of "Ancillary Businesses", not "Credit Rating Business", and are not subject to the regulations applicable to "Credit Rating Business" under the Financial Instruments and Exchange Act of Japan and its relevant regulation. PRC: Any SPO: (1) does not constitute a PRC Green Bond Assessment as defined under any relevant PRC laws or regulations; (2) cannot be included in any registration statement, offering circular, prospectus or any other documents submitted to the PRC regulatory authorities or otherwise used to satisfy any PRC regulatory disclosure requirement; and (3) cannot be used within the PRC for any regulatory purpose or for any other purpose which is not permitted under relevant PRC laws or regulations. For the purposes of this disclaimer, "PRC" refers to the mainland of the People's Republic of China, excluding Hong Kong, Macau and Taiwan.