OFR BRIEF SERIES
OFFICE OF FINANCIAL RESEARCH

24-05 | November 13, 2024

The Cyberattack on Change Healthcare: Lessons for Financial Stability

by Arthur Fliegelman and Daniel Stemp[1]

Cyberattacks are a growing threat to U.S. businesses, even with investments in cybersecurity. The U.S. financial system depends on technology for its operations. Even a brief outage of key services could have wide-ranging effects. While the financial system's cyber defenses have been strong so far, they can be improved by learning from recent attacks in other sectors. This brief examines the cyberattack on Change Healthcare, a critical service provider in healthcare. It also discusses how the U.S. financial system can better prepare for and reduce the risk of a similar attack on a systemically important firm.

Introduction

The financial system relies on uninterrupted service by many interconnected institutions and technology service providers.[2] Service outages, regardless of cause, can lead to immediate and serious financial system disruptions. Cyberattacks are of particular concern because they can be timed and targeted for maximum damage. In just the last 12 months, parts of the financial sector have experienced disruptions from cyberattacks at critical service providers (CSPs). The attacks on ICBC Financial Services, EquiLend, and Ongoing Operations are examples. In each case, the CSP was forced offline, and its customers were without access to its critical services for days to weeks. In each case, financial institutions implemented their business continuity plans to cope with the service outage. And in each case, the cyberattack revealed a CSP that was more critical to the financial sector than previously understood.[3] More frequent operational disruptions due to cyberattacks pose a growing systemic risk.[4]

Fortunately, none of the cyberattacks on the financial system have caused a major outage at a true single point of failure (SPoF) to the financial system. Other industries have not fared as well. The Colonial Pipeline attack disrupted fuel supply to the East Coast in 2021 and revealed the firm to be a SPoF. And in February 2024, an attack on Change Healthcare, the largest medical claims clearinghouse in the United States, disrupted critical operations and payment flows across the healthcare sector. Change Healthcare also provided technology solutions for essential back-office functions for healthcare providers.

As a clearinghouse, Change Healthcare has much in common with the financial market utilities (FMUs) and other CSPs on which the financial system relies. The Change Healthcare outage that occurred as a result of the firm's cyberattack underscores the far-reaching impact of a disruption at a CSP.

This brief examines lessons learned from the cyberattack on Change Healthcare and how these can be

applied to the financial system. During the outage, many healthcare providers that use Change Healthcare could not submit medical claims or receive payments. These providers included hospitals, physicians, and pharmacies. The service disruption strained cash flows and triggered a medical sector liquidity event. Healthcare providers' business continuity plans afforded some degree of operational resilience. Federal government support, somewhat similar to what has been used in the financial sector, mitigated the liquidity effects. Overall, the event highlights the importance of identifying potential SPoFs within the financial system and the economy and having robust plans for maintaining operations during service outages.

Change Healthcare is a SPoF in the U.S. Healthcare System

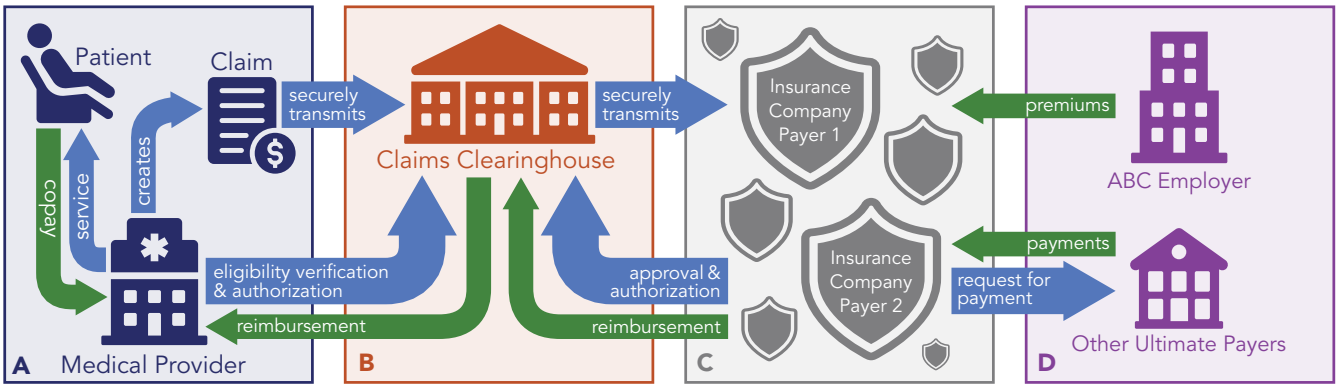
The U.S. healthcare system, like the financial system, has a network structure. They both have a multitude of service providers that securely exchange information. In healthcare, these providers include doctors' offices, hospitals, and pharmacies, and ultimate payers like insurance companies. Also included are many technology service providers that enable the exchange of information or automate almost every back-office and customer-facing function. The financial system similarly has numerous participants relying upon constant and rapid information flow that inform financial asset evaluation and the settlement of payments, for example. The financial system in particular relies on key providers to keep the system operating in a consistent and resilient manner, with generally little room for unexpected delay.

Claims clearinghouses like Change Healthcare play a critical role in the healthcare technology network. They manage and administer the healthcare authorization and payment system. Claims clearinghouses also perform vital functions, including confirming patients' insurance coverage, transferring claims and medical data, and facilitating payments for services rendered. In performing all these roles, clearinghouses are critical nodes that connect the many participants in the technology network (see **Figure 1**).

Before administering a service, medical providers must verify a patient's insurance eligibility and coverage. They do so by submitting an authorization request via a claims clearinghouse. This action is analogous to a debit card processor confirming a cardholder's bank balance before approving a transaction. Additionally, the medical provider may generate and submit a claim for payment using the clearinghouse's specialized software.

Change Healthcare is the largest medical claims clearinghouse in the United States. About 189 thousand medical providers use its software and services.[5] The

Figure 1. The Role of Claims Clearinghouses in the U.S. Healthcare System



Notes: A) Patients present their insurance cards, and the medical provider verifies coverage via claims clearinghouse. B) Claims clearinghouse reviews and processes the claim and forwards the claim to the payer. C) Insurers verify eligibility, approve, or reject claims, and reimburse medical providers through the claims clearinghouse. D) Employers pay premiums to insurance companies. Insurance companies may also act as administrators for self-insured organizations.

Source: Authors' creation

American Hospital Association (AHA) described it as the major source for "more than 100 critical functions that keep the healthcare system operating."[6] As a result, Change Healthcare touches one of every three patient records and handles $2 trillion in annual medical claims. This is estimated to be 44% of the funds that will flow through the U.S. medical system in 2024.[7]

These features give Change Healthcare a scale comparable to that of an FMU and make it a potential SPoF for the healthcare system. A court filing made by the Department of Justice quotes Change Healthcare as saying, "[The] healthcare system, and how payers and providers interact and transact, would not work without Change Healthcare."[8]

Like most FMUs, Change Healthcare provides a digital platform with strong network effects. As a clearinghouse, it stands in the middle of the many providers seeking to submit claims and the insurance companies seeking to pay claims. The more parties that use the same clearinghouse, the faster the claim can be processed and paid, which increases the value of the clearinghouse to its customers. As with most digital platforms, it has evolved over time to perform an expanded suite of technology solutions, making it a one-stop shop for many customers. Change Healthcare performs many functions similar to those of an FMU (see **Figure 2**).

The Cyberattack at Change Healthcare

On February 21, 2024, Change Healthcare discovered that a Russian-linked ransomware gang had breached its computer systems.[9] To mitigate the damage, Change Healthcare went offline. This effectively shut down the medical claims clearing process for a substantial portion of the medical sector. As of August 30, 2024, Change Healthcare reported that it was still attempting to restore some of its services.[10]

An AHA survey found 94% of hospitals affected financially by the attack. More than half of survey respondents said that the impact was "significant or serious."[11] A breakdown of the claims processing system severely affects the financial condition of U.S. healthcare providers. After the attack, Q1 2024 quarterly revenue for hospitals fell short of prior projections by 16.5% to 17.9%, according to Strata Decision Technology (see **Figure 3**).[12] By June 30, 2024, the smallest providers were still short about 7% of their expected Medicare revenue for the January to March 2024 period.[13]

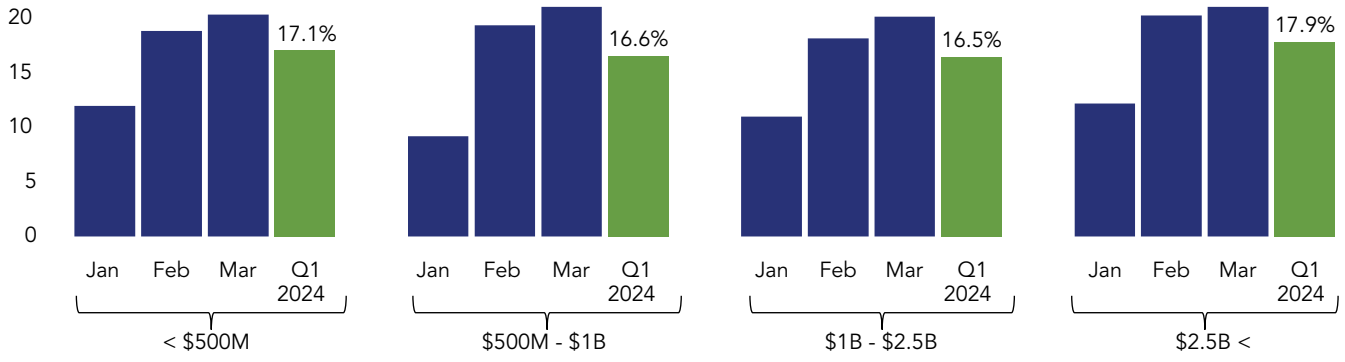
The Change Healthcare cyberattack may also cause substantial cyber insurance claims. Property Claims Services (PCS), an insurance industry data provider, labeled the attack as a cyber catastrophe, only the

Figure 2. Parallels Between Financial Market Utilities and Healthcare Claims Clearinghouses

Financial Sector Critical Functions	Healthcare Sector Critical Functions	Description
Clearing and Settlement	Claims Adjudication	Verifying and processing transactions in financial markets. In healthcare, clearinghouses adjudicate claims, checking for accuracy and facilitating payments between payers and providers.
Liquidity Provision	Cash Flow Facilitation	Ensuring sufficient cash flow in financial systems. In healthcare, clearinghouses maintain provider cash flow by speeding up claims processing.
Regulatory Reporting	Compliance and Reporting	Reporting transaction data for compliance in financial markets. In healthcare, clearinghouses check that claims data meet HIPAA patient information transmission standards.
Credit Risk Assessment	Insurance Eligibility Check	Evaluating counterparty risk before trades in financial markets. Healthcare clearinghouses verify patient insurance coverage before services are rendered to reduce non-payment risks for medical providers.

Source: Authors' creation

Figure 3. Hospitals Average Missing Share of Payments by Annual Operating Expense



Sources: Strata Decision Technology, Authors' analysis

second loss event to get that label. PCS defines a cyber catastrophe as an event with expected insured losses of over $250 million.[14] There might also be non-cyber insurance claims, including for business interruption and directors and officers liability insurance. However, most business losses would not be covered by any insurance.

The financial impact of the breach might be worse for other businesses than for Change Healthcare itself. According to S&P Global Ratings, the attack will not materially impact the credit rating of UnitedHealth Group, Change Healthcare's parent company.[15] However, many smaller and weaker medical providers have been severely affected by the cash flow disruption the cyberattack caused.[16] The American Medical Association found that 55% of doctors used their personal funds to cover their practice's expenses during the outage.[17] Fitch Ratings said that the cybersecurity incident at Change Healthcare could "negatively affect the credit profiles of smaller healthcare providers, pharmacies, and other companies that rely upon Change."[18] Smaller providers such as physician practices could have been substantially impacted as they often have limited liquidity and need the missing funds to pay for operational expenses, including payroll and supplies.[19]

To mitigate the cash flow issue from turning into a wider healthcare crisis and liquidity event with potential spillovers to the financial sector, the federal government provided support in various forms. The Centers for Medicare & Medicaid Services (CMS) advanced more than $3.2 billion to hospitals and other medical providers between March 9 and June 17.[20] CMS also asked private insurers to ease preauthorization requirements to reduce provider paperwork. UnitedHealth Group lent $6.5 billion to providers through April 30.[21] The combined $9.7 billion from these two programs was only about 2.6% of the roughly $375 billion in quarterly claims that Change Healthcare normally processes.[22] The level of financial assistance given to providers was likely inadequate, especially to small providers facing cash shortfalls.[23] In contrast, larger hospitals, which typically have four to ten months of cash reserves, fared better.[24] The financial sector lacks similar cash buffers to handle such disruptions.

Lessons Learned from the Cyberattack on Change Healthcare

The Change Healthcare cyberattack offers a case study about how such events at CSPs and potential SPoFs can affect downstream organizations. This attack began as a security breach on an unprotected server at a vital payment ecosystem participant. It then became a broader systemic problem for the healthcare sector. Emergency industry and federal government financial support mitigated the harm to patient care and the disruption of liquidity among healthcare providers. This section highlights three lessons learned with relevance for the financial sector and beyond.

Cyberattacks can disrupt liquidity, even when they occur outside the financial system.

Liquidity is a vital financial resource that keeps any organization operating. The Change Healthcare cyberattack substantially interrupted cash flow in the U.S. healthcare system for a considerable period. This then caused financial stress at a wide range of medical providers.

The Change Healthcare attack highlights the potential value of liquidity support outside the financial sector. In the case of Change Healthcare, UnitedHealth offered limited emergency liquidity to certain providers. Also, the federal government advanced limited emergency funds to certain Medicare healthcare providers. The combined funds that were advanced fell far short of the amounts needed to fully fund normal operations. This led to financial stress at many providers, which in a few cases resulted in providers ceasing operations or having to sell their businesses to another more financially stable operator.

Unlike the financial sector, where firm failures can trigger a chain reaction in which other firms close, healthcare provider failures typically don't cause widespread disruptions among related entities. However, the U.S. financial system is far less tolerant of major failures, especially among large, highly leveraged firms.

This provision of emergency funding resembles the Federal Reserve's provision of liquidity to the banking system. Banks can obtain short-term, collateralized loans from the Federal Reserve through the discount window. In recent years, the Federal Reserve also introduced various lending facilities to address other sources of extreme stress within the financial system.[25]

The Change Healthcare attack illustrates how a cyberattack at an FMU to the financial system could have serious and immediate repercussions. The U.S. financial system relies on a constant flow of funds between counterparties to settle trades and satisfy other obligations. A prolonged interruption in this process could require substantial emergency liquidity support from the official sector.

Vendor dominance and high transition costs amplify systemic risks.

When critical business functions depend on only one or a few vendors, there is a higher risk of broad disruptions if one vendor fails. Having a diverse set of vendors can help reduce this risk. If one vendor fails, other vendors can step in to meet the demand. Although using multiple vendors can be complex and expensive, it provides an immediate backstop if the main vendor fails. However, in many cases, it may be functionally impractical to have multiple vendors because of limited interoperability.

Part of what made the cyberattack on Change Healthcare so severe was that Change Healthcare had exclusivity clauses in its contracts with more than one-third of its clients. These clients were at high risk of business interruption when Change Healthcare's services became unavailable.[26]

Some payers had no backup payment system and depended entirely on Change Healthcare. Change Healthcare's "managed gateway" payer clients only used Change Healthcare to process provider's claims.[27] They had no automated way to process claims once Change Healthcare suspended its operations. This severely crimped providers' cash flows.

Additionally, exclusivity contracts prevented other clearinghouses from connecting to payers that only accepted claims through Change Healthcare. Even clients of competitive clearinghouses were affected because of these exclusivity requirements. Change Healthcare did waive its exclusivity clauses, possibly in part due to pressure from insurance regulators.[28] However, switching to a new claims clearinghouse is a costly and time-consuming process.[29]

Operational resilience is critical.

Operational resiliency is crucial for an organization to continue functioning despite disruptions. Organizations need well-prepared and practiced business continuity plans that can be activated quickly during internal issues or external service interruptions at a CSP. Developing these plans requires forethought and flexibility, as workarounds may be less efficient but still allow operations to proceed. These strategies

might involve manual processes or switching to alternative service providers, but the key is ensuring that operations do not stop.

Change Healthcare lacked resiliency in the form of a recovery plan with well-rehearsed procedures to minimize downtime. Its history of growth through acquisitions may have contributed to this vulnerability. Integrating disparate acquired systems poses substantial technological challenges. These challenges complicate and divert resources from cybersecurity planning. Growth through acquisitions is a common strategy in many sectors, including the financial sector.

Change Healthcare had data backups, but those backups were not properly isolated from the compromised network and were in turn affected by the breach. A compromised backup is not a functional backup.

As a result of the outage, Change Healthcare lost access to critical information. Change Healthcare could no longer communicate with clients, providers, and other stakeholders.

Coordinating mitigation efforts and maintaining network stability is essential when a central network node goes offline. The financial system might tolerate brief FMU service interruptions if robust communication reassures stakeholders that service will be restored promptly.[30] For major central counterparties, the standard recovery time objective after an operational failure is two hours or less.[31] Rapid and accurate communication after a cyberattack is an important aspect to recovery.

The financial sector is likely better prepared than other sectors in terms of business continuity planning. Regulations emphasize the importance of reliable and tested data backups for restoring functionality.[32] Shared backup facilities like Sheltered Harbor offer a robust solution.[33] Reciprocal backup agreements and cloud-based solutions may be more practical for smaller firms.[34] Cost-effective robust business continuity plans is essential for improving financial stability.

Conclusion

Networks such as the U.S. financial system can be highly dependent upon one or a few CSPs. These networks can be at high risk of operational disruptions when even one provider is down. Interruptions often occur because of an external cyberattack but they can also be the result of operational failures.

When interruptions occur, it is important: (1) that the CSP has an effective business continuity plan to continue its operations to the maximum extent possible; (2) that affected downstream organizations have their own business continuity plans so they too can continue operating; and (3) that the stricken CSP has a plan to restore normal operations on a timely basis.

The more dominant a CSP's role, the more important it becomes that the CSP has an effective business continuity plan that can be readily implemented. FMUs by definition have a vital role in the U.S. financial system. Consequently, FMUs are expected to have a high level of cybersecurity combined with effective business continuity plans.

However, it has become clear that other, less dominant organizations, may play more important roles in the financial system than previously thought. The role of these vendors was only fully realized when their operations were disrupted. Within the financial sector, examples include ICBC Financial Services, EquiLend, and Ongoing Operations.

The Change Healthcare incident illustrates how interruptions outside of the financial system can have liquidity effects in nonfinancial sectors of the economy. If not mitigated, such liquidity events could result in higher default rates on nonfinancial business debt, stressing financial institutions and perhaps the broader financial system. Fortunately, in this case, support from UnitedHealth and CMS helped contain the damage from extending beyond the healthcare system. Without this financial aid, business failures in the healthcare sector and their knock-on effects could have more broadly affected patient care and the wider U.S. economy.

So far, the U.S. financial system has avoided a long-lasting technology outage with effects as severe and far-reaching as those occurring in healthcare from the Change Healthcare cyberattack. However, as the financial system's reliance on technology grows, such an event becomes more likely.

Endnotes

1 Arthur Fliegelman, Senior Financial Analyst, Office of Financial Research (Arthur.Fliegelman@ofr.treasury.gov) and Daniel Stemp, Senior Financial Analyst, Office of Financial Research (Daniel.Stemp@ofr.treasury.gov).

2 The authors wish to thank the College of Healthcare Information Management Executives (CHIME) and Chelsea Arnone for their assistance in the preparation of this report.

3 For an analysis of how financial institutions dealt with an earlier cyberattack on a CSP, see: Antonis Kotidis and Stacey L. Schreft, "Cyberattacks and Financial Stability: Evidence from a Natural Experiment," Finance and Economics Discussion Series (FEDS) no. 2022-025 (Board of Governors of the Federal Reserve System, May 2022), https://www.federalreserve.gov/econres/feds/cyberattacks-and-financial-stability-evidence-from-a-natural-experiment.htm.

4 Annual Report 2023 (Financial Stability Oversight Council, 2023), https://home.treasury.gov/system/files/261/FSOC2023AnnualReport.pdf.

5 William Altman, Ethan Spangler, and John Laux, "The Change Healthcare Attack: Quantifying Footprint for Cyber (Re)insurers," CyberCube, undated blog post, https://insights.cybcube.com/en/the-change-healthcare-attack-quantify-footprint-for-cyber-reinsurers.

6 "AHA Letter to House E&C Subcommittee for May 1 Hearing on Change Healthcare Cyberattack," American Hospital Association, April 29, 2024, https://www.aha.org/lettercomment/2024-04-29-aha-letter-house-ec-subcommittee-may-1-hearing-change-healthcare-cyberattack

7 "AHA Letter to House E&C Subcommittee for May 1 Hearing on Change Healthcare Cyberattack," American Hospital Association, April 29, 2024, https://www.aha.org/lettercomment/2024-04-29-aha-letter-house-ec-subcommittee-may-1-hearing-change-healthcare-cyberattack

8 Department of Justice filing, February 24, 2022, https://www.justice.gov/atr/case-document/file/1476901/dl.

9 TechTarget Editorial Staff, "Change Healthcare Cyberattack Fallout Continues," TechTarget, May 2, 2024, https://healthitsecurity.com/news/change-healthcare-disconnects-system-amid-cyberattack.

10 "Information on the Change Healthcare Cyber Response," Change Healthcare, September 3, 2024, https://www.unitedhealthgroup.com/ns/changehealthcare.html.

11 "AHA Survey: Change Healthcare Cyberattack Significantly Disrupts Patient Care, Hospitals' Finances," American Hospital Association, February 21, 2024, https://www.aha.org/2024-03-15-aha-survey-change-healthcare-cyberattack-significantly-disrupts-patient-care-hospitals-finances.

12 "Healthcare Performance Trends Report: Q2 2024," Strata Decision Technology, August 9, 2024, https://www.stratadecision.com/quarterly-healthcare-performance-trends-report/.

13 "Performance Trends Report: Second Quarter 2024," Strata Decision Technology, Second Quarter 2024, https://www.syntellis.com/sites/default/files/2024-08/performance_trends_aug_hc.1132.08.24.pdf.

14 Steve Evans, "PCS Designates Change Healthcare & MOVEit as Cyber Catastrophe Loss Events," Artemis, April 29, 2024, https://www.artemis.bm/news/pcs-designates-change-healthcare-moveit-as-cyber-catastrophe-loss-events/.

15 Francesca Mannarino and James Sung, "Bulletin: Cyber Attack at Change Healthcare Poses Reputational Risks for UnitedHealth Group Inc. Uncertainties Remain," S&P Global Ratings, March 11, 2024, https://disclosure.spglobal.com/ratings/en/regulatory/article/-/view/type/HTML/id/3136919.

16 Kailash Chhaya et al., "Providers Continue to Suffer Disruption from Change Healthcare Attack," Moody's Investors Service, March 8, 2024, https://www.moodys.com/research/Healthcare-US-Providers-continue-to-suffer-disruption-from-Change-Healthcare-Sector-Comment--PBC_1400730; and Steven Bisciello et al., "The Change Healthcare Data Breach and Navigating Your Exposure," Eisner Amper, March 13, 2024, https://www.eisneramper.com/insights/health-care/change-healthcare-data-breach-navigate-exposure-0324/.

17 "Change Healthcare Cyberattack Impact," American Medical Association, 2024, https://www.ama-assn.org/system/files/change-healthcare-survey-results.pdf.

18 "Change's Cyber Security Incident May Affect Smaller Healthcare Issuers," Fitch Ratings, March 18. 2024, https://www.fitchratings.com/research/insurance/changes-cyber-security-incident-may-affect-smaller-healthcare-issuers-18-03-2024.

19 Mike Bradley, "Outages from Change Healthcare Cyberattack Causing Financial 'Mess' for Doctors," CNBC, March 1, 2024, https://www.nbcnews.com/news/us-news/outages-change-healthcare-cyberattack-causing-financial-mess-doctors-rcna141321.

20 "CMS Preparing to Close Program that Addressed Medicare Funding Issues Resulting from Change Healthcare Cyber-Attack," Centers for Medicare & Medicaid Services, June 17, 2024, https://www.cms.gov/newsroom/press-releases/cms-preparing-close-program-addressed-medicare-funding-issues-resulting-change-healthcare-cyber.

21 UnitedHealth Group Incorporated, Form 10-Q, March 31, 2024, https://www.unitedhealthgroup.com/content/dam/UHG/PDF/investors/2024/UNH_Q1-2024_Form-10-Q.pdf.

22 "A Trusted Advisor to the Healthcare System," Change Healthcare, 2021. Retrieved August 21, 2024, from https://www.changehealthcare.com/content/dam/change-healthcare/sales---marketing-content/payer-and-provider/corporate-content/brochure/corporate-overview-brochure/corporate_overview.pdf.

23 Matthew Cahill and Dean Ungar, "Providers continue to suffer disruption from Change Healthcare cyberattack," Moody's Ratings, https://www.moodys.com/research/Healthcare-US-Providers-continue-to-suffer-disruption-from-Change-Healthcare-Sector-Comment--PBC_1400730; and "Change Healthcare cyberattack," American Medical Association, May 24, 2024, https://www.ama-assn.org/practice-management/sustainability/change-healthcare-cyberattack.

24 S&P Global Ratings, "U.S. Not-For-Profit Health Care Stand-Alone Hospital Median Financial Ratios—2023," August 7, 2024, https://www.spglobal.com/ratings/en/research/articles/240807-u-s-not-for-profit-health-care-stand-alone-hospital-median-financial-ratios-2023-13207056.

25 For example: the Bank Term Funding Program (BTFP) in 2023; and the Commercial Paper Funding Facility (CPFF), Primary Dealer Credit Facility (PDCF), and Term Asset-Backed Securities Loan Facility (TALF) in 2020.

26 Steve Alder, "Senators Grill UHG CEO About Change Healthcare Cyberattack," The HIPAA Journal, May 3, 2024, https://www.hipaajournal.com/change-healthcare-responding-to-cyberattack/; and Senator Ron Wyden's opening comments to Senate Committee on Finance hearing "Hacking America's Health Care: Assessing the Change Healthcare Cyber Attack and What's Next," May 1, 2024, https://www.finance.senate.gov/chairmans-news/wyden-hearing-statement-on-change-healthcare-cyberattack-and-unitedhealth-groups-response.

27 "Proposed Findings of Fact and Conclusions of Law of Defendants UnitedHealth Group Incorporated and Change Healthcare Inc.," September 7, 2022, https://appliedantitrust.com/14_merger_litigation/cases_doj/unitedhealth_change2022/1_ddc/unitedhealth_change_ddc_pff_def2022_09_07redacted.pdf.

28 Mike Kreidler, "Third Notification Regarding Change Healthcare Cybersecurity Event," State of Washington Office of Insurance Commissioner, April 15, 2024, https://www.

insurance.wa.gov/sites/default/files/documents/OIC%20Letter%20to%20Industry%20regarding%20Change%20Healthcare%2004152024.pdf.

29 "Change Healthcare Cyberattack Impact," American Medical Association, 2024, https://www.ama-assn.org/system/files/change-healthcare-survey-results.pdf

30 Ann Saphir, "Fedwire Resumes Operations After Hours Long Disruption," Reuters, February 24, 2021, https://global.factiva.com/redir/default.aspx?P=sa&an=LBA0000020210224eh2o04chd&drn=drn%3aarchive.newsarticle.LBA0000020210224eh2o04chd&cat=a&ep=ASE.

31 CCPView Clarus Financial Technology.

32 Ivet Petrova, "Disaster Recovery Compliance in the Financial Sector: How a Managed Service Provider Can Help," Cloudflare, July 21, 2023, https://cloudscale365.com/disaster-recovery-compliance-in-the-financial-sector-how-a-managed-service-provider-can-help/.

33 For additional information on Sheltered Harbor and its role in the banking system, see https://shelteredharbor.org/.

34 FFIEC IT Examination Handbook Infobase, https://ithandbook.ffiec.gov/it-booklets/business-continuity-management/v-business-continuity-plan/vc-facilities-and-infrastructure/vc1-data-center-recovery-alternatives/.