DXC TECHNOLOGY

Banking and Capital Markets bi-weekly news round-up

21 July 2023
Edition no: 293

Welcome to the DXC-curated news round-up.

A collection of technology-related articles for banking and capital markets (BCM). DXC Technology (NYSE: DXC) helps global companies run their mission-critical systems and operations while modernizing IT, optimizing data architectures, and ensuring security and scalability across public, private and hybrid clouds.

With this news round-up, published every 2 weeks, we highlight innovative and emerging news, regulation and research, as well as including DXC Technology's thought leadership that explores new ideas, technologies and best practices.

To thrive in the complex and competitive financial market, banking and capital markets firms need products and services that work for twenty-first century customers and meet regulatory obligations. Modernise your IT and transform your business with DXC Technology's IT services and robust partner ecosystem.

Should you have any comments or suggestions, please feel free to contact me.

Happy reading.

Jean-Paul Simoes

Director of Banking and Capital Markets (BCM) Compliance, DXC Technology

jean-paul.simoes@dxc.com

DXC Technology Banking and Capital Markets bi-weekly news round–up

Contents

DXC Technology Banking and Capital Markets bi-weekly news round–up

Artificial Intelligence (AI)

Use of AI in finance likely to trigger rise in fraud, says UK watchdog

Reuters: Applying artificial intelligence (AI) to financial services must go hand-in-hand with better fraud prevention and resilience to hacking and outages, Britain's Financial Conduct Authority (FCA) was expected to say on July 12.

Nikhil Rathi, chief executive of the FCA, said in remarks made available to the media in advance of a speech, that he was already seeing AI-based business models requesting authorisation. AI's use can benefit markets, such as cutting prices for consumers, but also cause imbalances if "unleashed unfettered", per Rathi.

"This means that as AI is further adopted, the investment in fraud prevention and operational and cyber resilience will have to accelerate simultaneously," per Rathi.

"We will take a robust line on this – full support for beneficial innovation alongside proportionate protections. We will remain super vigilant on how firms mitigate cyber-risks and fraud given the likelihood that these will rise." The watchdog has already observed how volatility during the trading day has doubled and amplified compared to during the 2008 global financial crisis.

DXC's Perspective

It surely makes sense to ramp up risk controls as AI is more widely adopted – as it would with any emerging technology. But there is no reason to assume that the net result of AI will be a rise in fraud, not least because many of the applications of AI in financial services are to reduce fraud, for example, by identifying anomalous patterns for fraud, KYC, and insider trading. The example of preventing push-payment fraud in the article below is a case in point.

David Rimmer
Industry Advisor – BCM
DXC Technology

Mastercard's New AI Tool Helps Nine British Banks Tackle Scams

Bloomberg: Mastercard Inc. is selling a new artificial intelligence-powered tool that helps banks more effectively spot if their customers are trying to send money to fraudsters.

Nine of the UK's biggest banks, including Lloyds Banking Group Plc, Natwest Group Plc and Bank of Scotland Plc, have signed up to use the Consumer Fraud Risk system, Mastercard told Bloomberg News.

Trained on years of transaction data, the tool helps to predict whether someone is trying to transfer funds to an account affiliated with "authorized push payment scams." This type of fraud involves tricking a victim into moving money into an account falsely posing as a legitimate payee, such as a family member, friend, or a business.

The tool comes as UK banks prepare for new rules from the Payment Systems Regulator that will require them to compensate customers affected by APP scams from 2024. Historically banks haven't been liable for this type of fraud, although some signed a voluntary agreement to pay back victims.

DXC Technology Banking and Capital Markets bi-weekly news round–up

Class-Action Lawsuit for Scraping Data without Permission

Schneier.com: I have mixed feelings about this class-action lawsuit against OpenAI and Microsoft, claiming that it "scraped 300 billion words from the internet" without either registering as a data broker or obtaining consent. On the one hand, I want this to be a protected fair use of public data. On the other hand, I want us all to be compensated for our uniquely human ability to generate language.

There's an interesting wrinkle on this. A recent paper showed that using AI generated text to train another AI invariably "causes irreversible defects." From a summary:

The tails of the original content distribution disappear. Within a few generations, text becomes garbage, as Gaussian distributions converge and may even become delta functions. We call this effect model collapse.

Just as we've strewn the oceans with plastic trash and filled the atmosphere with carbon dioxide, so we're about to fill the Internet with blah. This will make it harder to train newer models by scraping the web, giving an advantage to firms which already did that, or which control access to human interfaces at scale. Indeed, we already see AI startups hammering the Internet Archive for training data.

Achieving Sensible AI Regulation

Debevoise & Plimpton: At its core, the SIFMA approach would require companies, under the supervision of their sectoral regulators, to (1) identify how AI is being used, (2) determine which AI uses pose the highest risks, (3) have qualified persons or committees at the company review high-risk AI applications and determine whether the risks are too high, and if so, (4) provide meaningful mitigation steps to reduce those risks to an acceptable level or require that the AI application be abandoned.

SIFMA's risk-based approach to AI regulation would provide a valuable, flexible framework through which companies and their sectoral regulators can build tailored AI governance and compliance programs that ensure accountability and trust without stifling innovation or wasting time or resources on low-risk AI applications.

The proliferation of AI tools and rapid pace of AI adoption have led to calls for new regulation at all levels.

As the leading industry trade association representing broker-dealers, investment banks, and asset managers operating in the U.S. and global capital markets, SIFMA has proposed a practical, risk-based approach to regulating AI that contains strong accountability measures for high-risk AI uses, while providing flexibility to allow industry to innovate.

DXC's Perspective

The SIFMA proposals at first sight align with the EU AI Act which is also risk-based. The key issue, however, will be the definition of risk. The EU, for example, defines high risk as "significant harm to people's health, safety, fundamental rights or the environment." Will SIFMA take a comparable view of risk, or limit itself to financial risk or operational risk?

David Rimmer
Industry Advisor – BCM
DXC Technology

DXC Technology Banking and Capital Markets bi-weekly news round–up

FTC investigates OpenAI over data leak and ChatGPT's inaccuracy

Washington Post: The Federal Trade Commission has opened an expansive investigation into OpenAI, probing whether the maker of the popular ChatGPT bot has run afoul of consumer protection laws by putting personal reputations and data at risk.

The agency last week sent the San Francisco company a 20-page demand for records about how it addresses risks related to its AI models, according to a document reviewed by The Washington Post. The salvo represents the most potent regulatory threat to date to OpenAI's business in the United States, as the company goes on a global charm offensive to shape the future of artificial intelligence policy.

Analysts have called OpenAI's ChatGPT the fastest-growing consumer app in history, and its early success set off an arms race among Silicon Valley companies to roll out competing chatbots. The company's chief executive, Sam Altman, has emerged as an influential figure in the debate over AI regulation, testifying on Capitol Hill, dining with lawmakers and meeting with President Biden and Vice President Harris.

Cybersecurity

Cybersecurity stocktake exposes gaps

The Australian Prudential Regulation Authority (APRA) has released some early findings from an expansive study that it is conducting on cyber resilience in financial services.

As part of this study, APRA's regulated entities are required to appoint an independent auditor to assess their compliance with prudential standard CPS 234 Information Security, which seeks to ensure that regulated entities have baseline prevention, detection, and response capability to withstand cyber security threats. APRA states that results from this first tranche of assessments highlight several concerning gaps across the industry.

The most common gaps identified in this tranche were:

- incomplete identification and classification for critical and sensitive information assets;
- limited assessment of third-party information security capability;
- inadequate definition and execution of control testing programs;
- incident response plans not being regularly reviewed or tested;
- limited internal audit review of information security controls; and
- inconsistent reporting of material incidents and control weaknesses to APRA in a timely manner.

DXC Technology Banking and Capital Markets bi-weekly news round–up

Who are the ransomware gangs wreaking havoc on the world's biggest companies?

The Guardian: In the past year, some of the UK's most recognised institutions, from the Guardian to Royal Mail, have been hit with the defining cybercrime of our time: ransomware. Hackers locking up computer networks and demanding payment for the keys to restore them have snarled operations and left victims scrambling to recover.

Nearly every sector of society, including healthcare, business, government**,** and education, has now been targeted by ransomware gangs making demands that stretch into the tens of millions. Ironically, just a few months before the release of my own book on ransomware, my publisher was hit with a bruising attack, leaving my co-author and I unable to reach our editors via phone or email.

In the UK over the past few weeks alone, separate attacks have reportedly compromised NHS employee records and confidential emails, as well as data on more than 1 million patients. In the US, a baby's death was attributed to a 2019 ransomware attack on an Alabama hospital that knocked out monitors displaying foetal heart-rate tracing information at a nurses' station.

NYDFS Publishes Revised Amendments to Its Cybersecurity Regulation – What Got Fixed, and What Still Needs Fixing

Debevoise & Plimpton: In this Debevoise Data Blog post, we discuss the changes reflected in the Revised Amendment and what additional changes the NYDFS should consider before issuing its final amendment. Highlights include:

- narrowing the definition of Class A companies;
- removing some of the external requirements for audits and risk assessments;
- softening the cyber expertise requirement for boards;
- removing the internal reporting requirement for material issues found during penetration testing;
- significantly increasing the MFA requirements;
- narrowing the scope of incident response and business continuity plans;
- adding a materiality threshold for both violations and certifications of compliance;
- responding to requests for clarification; and
- changing the effective dates for certain requirements.

Companies or trade groups considering making comments on the Revised Amendment should carefully review the 92-page Assessment of Public Comments that NYDFS released explaining why it accepted certain comments and rejected others.

Regulatory

China ends probe of Ma-backed Ant with $984 million fine

Accessing the article may require a subscription.

American Banker: Chinese regulators imposed a 7.12 billion yuan ($984 million) fine on Ant Group, according to a statement from the central bank, wrapping more than two years of probes into the finance technology giant founded by billionaire Jack Ma.

The People's Bank of China said it imposed fines on Ant Group and its subsidiaries, including confiscation of illegal income, according to a statement on Friday. The sanctions were in response to violations of laws and regulations in areas including financial consumer protection, payment and settlement business and anti-money laundering obligation in the past years, the statement showed.

The move draws a line under the multi-year crackdown that torpedoed Ant's record initial public offering in 2020 and ensnared some of the nation's most powerful private firms in sectors from online education to gaming. It paves the way for Ant to revive growth and even eventually resurrect plans for an IPO.

Ant Group said it has completed rectification required by China's financial regulators, according to a company statement.

Bank of America to pay over $250 million over junk fees, other issues

Reuters: Bank of America on July 11 agreed to pay $250 million in fines and compensation to settle claims the bank systematically double-charged customers fees, withheld promised credit card perks, and opened accounts without customer authorization.

Bank of America agreed to pay $100 million in restitution to harmed consumers and another $150 million in civil penalties after the Consumer Financial Protection Bureau (CFPB) and Office of the Comptroller of the Currency (OCC) said the bank violated a number of laws beginning in 2012.

Bank of America reaped hundreds of millions of dollars by charging multiple fees to customers who did not have enough funds in their accounts from February 2018 until February 2022, the CFPB said in a statement. Consumers could not reasonably expect or understand they would be hit with $35 fees each time the bank declined to pay a single transaction, regulators said.

In a statement, Bank of America said it voluntarily eliminated or reduced a range of fees last year.

Other DXC BCM News

Webinar: Digitisation and data trends that are defining the future of banking and building societies

On 3 August, DXC is hosting a virtual webinar on "Digitisation and Data Trends That Are Defining the Future of Banks and Building Societies." Join financial services experts Andy Haigh and Jeremy Donaldson from DXC Technology to learn how data-driven technologies can help financial services organizations transform customer experience and automate repeated processes. **Register now.**

Webinar: Driving Digital Transformation for Financial Services with Observability and App Modernization

On 7 September, DXC is hosting a virtual webinar on "Driving Digital Transformation for Financial Services with Observability and App Modernization." In partnership with Dynatrace. Join financial services experts from DXC and Dynatrace to learn to learn how to achieve operational resilience with shift-left powered by Dynatrace and DXC. **Register now.**

Developing a data strategy in banking and capital markets

Data is king. Banks that know how to effectively harness it, manage it and monetize it can derive far better business insights, create significant growth opportunities and stay ahead of regulatory demands. Huge benefits can be reaped by developing a clear data strategy that defines how to access, ingest and connect the essential data that can drive positive business outcomes. **Read DXC's latest paper** to learn about how banks can get the most out of their data.

Executive Data Series: The banking customer in a data-rich world

In the latest conversation of the Executive Data Series, DXC's Head of Banking and Capital Markets (EMEA) Andy Haigh sits down with Mohammed 'Khal' Khalid to discuss how banks can use data and analytics to transform financial services and improve the customer experience. **Listen to the full conversation (23 mins.) or read the transcript:** https://dxc.to/3NlsbXI

DXC Technology Banking and Capital Markets bi-weekly news round–up

Should you have any questions on the round-up or a particular topic, please feel free to contact your DXC representative.

Learn more at:
dxc.com/banking

Subscribe to this report at:
https://connect.dxc.technology/DXC-BCM-News.html

Disclaimer

All statements in this communication that do not directly and exclusively relate to historical facts constitute "forward-looking statements." These statements represent current expectations and beliefs, and no assurance can be given that any goal, plan, or result set forth in any forward-looking statement can or will be achieved, and readers are cautioned not to place undue reliance on such statements which speak only as of the date they are made. Such statements are subject to numerous assumptions, risks, uncertainties, and other factors that could cause actual results to differ materially from those described in such statements, many of which are outside of our control. For a written description of these factors, see the section titled "Risk Factors" in DXC's Annual Report on Form 10-K for the fiscal year ended 31 March 2023, and any updating information in subsequent SEC filings. We do not undertake any obligation to update or release any revisions to any forward-looking statement or to report any events or circumstances after the date of this press release or to reflect the occurrence of unanticipated events except as required by law.

DXC Technology
DXC.com

About DXC Technology

DXC Technology (NYSE: DXC) helps global companies run their mission-critical systems and operations while modernizing IT, optimizing data architectures, and ensuring security and scalability across public, private and hybrid clouds. The world's largest companies and public sector organizations trust DXC to deploy services to drive new levels of performance, competitiveness, and customer experience across their IT estates. Learn more about how we deliver excellence for our customers and colleagues at **DXC.com**.