acxell

ADVISOR

Winter 2024

LEARN FROM PAST MISTAKES
"Postmortems" on failed institutions are instructive for community banks

7 WAYS AI IS TRANSFORMING THE BANKING INDUSTRY

WHAT CAN VISUAL ANALYTICS DO FOR YOUR BANK?

BANK WIRE

acxell

www.acxellrms.com 877.651.1700

LEARN FROM PAST MISTAKES

"Postmortems" on failed institutions are instructive for community banks

In the aftermath of three notable bank failures in 2023, federal banking regulators issued comprehensive reports detailing the underlying causes of those failures. These postmortems are must-reads for banks of all sizes because they point out management shortcomings that led to the bank failures — as well as regulators' plans to become more proactive in addressing bank risks. Here are some highlights of the three reports.

1. SILICON VALLEY BANK

According to the Federal Reserve (Fed) report, Silicon Valley Bank (SVB) was "a textbook case" of bank mismanagement. Its senior leadership failed to manage basic interest rate and liquidity risk, which led to a run by depositors. The causes of SVB's failure were tied to 1) its business model, which was highly concentrated in early-stage and start-up technology companies and relied heavily on uninsured deposits, and 2) its failure to sufficiently address interest rate and liquidity risk. These factors left SVB "acutely exposed to the specific combination of rising interest rates and slowing activity in the technology sector that materialized in 2022 and early 2023," observed the Fed. Also, SVB had accumulated substantial unrealized losses on available-for-sale (AFS) securities.

In addition to the fact that SVB's directors didn't receive adequate risk-related information from management, SVB:

- Didn't hold management accountable for effective risk management,
- Failed its own internal liquidity stress tests and had no workable plan to access liquidity in times of stress, and
- Managed interest rate risk with a focus on short-term profits, rather than on managing long-term risks and the risk of rising rates.

The Fed also took some of the blame, noting that supervisors didn't fully appreciate the extent of SVB's vulnerabilities as it grew rapidly in size and complexity. Thus, it failed to take sufficient steps to ensure that SVB addressed those problems quickly.

2. SIGNATURE BANK

According to the Federal Deposit Insurance Corporation (FDIC) postmortem, the primary cause of Signature Bank's failure was "illiquidity precipitated by contagion effects in the wake of" deposit runs that led to the failure of SVB and the self-liquidation of Silvergate Bank. The FDIC noted other causes of Signature Bank's failure included its:

- Pursuit of "rapid, unrestrained growth" without developing risk management practices and controls appropriate for its size and complexity,
- Failure to prioritize good corporate governance and heed FDIC examiner concerns,

- Overreliance on uninsured deposits to fund its rapid growth, without implementing fundamental liquidity risk management practices and controls, and
- Failure to understand the risks associated with reliance on cryptocurrency deposits.

Like the Fed, the FDIC accepted some responsibility for Signature Bank's failure, noting that it "could have escalated supervisory actions sooner," its "examination work products could have been timelier," and it could have communicated more effectively with the bank's board and management.

3. FIRST REPUBLIC BANK

According to the FDIC, First Republic Bank failed primarily because of "a loss of market and depositor confidence" in the wake of the SVB and Signature Bank failures, resulting in a bank run. Notably, the FDIC found that First Republic Bank was well run, responsive to supervisory feedback, and implemented appropriate infrastructure, controls and risk management processes as it grew. Nevertheless, specific attributes of its business model and management strategies made it vulnerable to interest rate changes and the contagion effects of previous bank failures, including:

- Rapid growth,
- Loan and funding concentrations,
- Overreliance on uninsured deposits and depositor loyalty, and
- Failure to sufficiently mitigate interest rate risk.

Again, the FDIC examined its own possible role in First Republic Bank's failure. Although it was unclear whether earlier supervisory action would have made a difference, the report noted that "meaningful action to mitigate interest rate risk and address funding concentrations would have made the bank more resilient and less vulnerable."

ROLE OF SOCIAL MEDIA IN LIQUIDITY RISK

An interesting takeaway from the regulators' postmortems (see main article) is the role that social media, together with banking technology, plays in liquidity risk. In its postmortem on Silicon Valley Bank (SVB), the Federal Reserve (Fed) commented that "social media enabled depositors to instantly spread concerns about a bank run, and technology enabled immediate withdrawals of funding."

On March 8, 2023, for example, SVB announced a balance sheet restructuring, including a sale of certain securities and an intention to raise capital. The next day, SVB experienced deposit outflows totaling over $40 billion, as uninsured depositors, interpreting the announcement as a signal of financial distress, began withdrawing their funds "in a coordinated manner with unprecedented speed." According to the Fed, the run appeared to be fueled by social media and the bank's concentrated network of venture capital investors and technology firms.

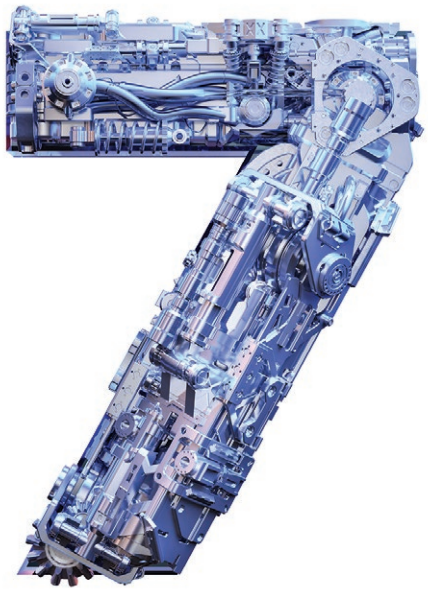
STAY TUNED

To help avoid future bank failures, regulators are considering several changes, including rethinking stress testing requirements; imposing additional capital or liquidity requirements on banks with inadequate capital planning, liquidity risk management, or governance and controls; incorporating unrealized losses and gains into regulatory capital rules; and encouraging banks to avoid concentrations on both sides of the balance sheet.

The extent to which these changes will trickle down to community banks is uncertain. But expect greater regulatory scrutiny in the future, particularly with respect to capital, liquidity risk and interest rate risk. ■

7 WAYS AI IS TRANSFORMING THE BANKING INDUSTRY

Artificial intelligence (AI) is impacting businesses in virtually every industry today, and banking is no exception. Banks of all sizes increasingly recognize AI's potential to help them improve efficiency, reduce costs, enhance the customer experience and combat fraud. Here are seven examples of how banks are using AI:



1. Customer service. Banks are using natural language processing and other AI applications to create conversational interfaces, or "chatbots," that can improve the customer experience. These applications are available to customers 24/7. Plus, with access to troves of data and the ability to learn about specific customers' behavior and usage patterns, they can offer highly personalized customer support at a fraction of the cost, and often more effectively, than humans.

Among other things, chatbots can answer account inquiries, reset passwords, assist with fund transfers and automatic payments, and assist with loan applications. Some banks also are using AI to recommend financial services and products, though the Consumer Financial Protection Bureau (CFPB) has been critical of the use of AI and chatbots in underwriting in some instances.

2. Fraud prevention and detection. Traditional approaches to combating fraud are becoming more challenging due to the number of daily transactions and the many customer behaviors that need to be monitored to identify anomalies. AI applications can quickly detect even subtle deviations from customers' usual account activity and behavior patterns. These trends can alert bank personnel to potentially fraudulent activities that warrant further investigation.

AI also has the ability to monitor bank systems and provide early warnings of cyberthreats, enabling bank personnel to respond quickly and minimize the damage. Examples of cyberattacks include phishing scams, ransomware and other malware, and identity theft.

3. Underwriting decisions. Banks are beginning to use AI to improve their loan and credit decisions. AI-based systems are able to sift through vast amounts of data to analyze customer behavior and activity patterns that evince creditworthiness. They can also help spot, and flag, behaviors or characteristics that might increase the chances an applicant will default.

4. Collections. By analyzing customer data, AI can spot warning signs that indicate potential delinquencies or defaults. It also can communicate with customers and offer personalized solutions for helping them get current on their payments and avoid default.

5. Automation. Strictly speaking, robotic process automation (RPA) isn't AI, but it has a similar impact

on banking processes. RPA refers to software tools that automate time-consuming, repetitive tasks.

Not only does RPA free up bank personnel to focus on higher-value activities, but it also can improve productivity and reduce errors. Examples of the many uses of RPA include inputting data and documents, opening accounts, and processing address changes. In addition, it can be used to automate and standardize many tasks related to customer communications and regulatory compliance.

6. BSA/AML compliance. AI can be invaluable to Bank Secrecy Act/Anti-Money Laundering (BSA/AML) compliance efforts. It can sift through enormous amounts of transaction data and identify suspicious activities that would be difficult, if not impossible, to detect using traditional methods.

7. Marketing. By processing and analyzing huge amounts of data, AI can help banks track and even predict market trends. And by collecting data about a bank's customers, it can reveal untapped sales and cross-selling opportunities.

HERE TO STAY

For banks interested in taking advantage of AI, significant challenges remain, including implementing and maintaining the systems and the extensive data needed to support it. However, as this technology becomes more commonplace and cheaper, its benefits will be difficult to ignore. ■

WHAT CAN VISUAL ANALYTICS DO FOR YOUR BANK?

Criminals are continuously looking for ways to use rapidly advancing technology for their own nefarious purposes. This is an ongoing issue for many community banks as they try to prevent money laundering and other crimes from happening within their operations. To protect your bank from criminal infiltration and ensure your bank remains in compliance with Bank Secrecy Act/Anti-Money Laundering (BSA/AML) laws and regulations, it's best to fight fire with fire. Consider using data visualization software to help detect possible crimes before they can take hold.

HOW TO COMPLY WITH BSA/AML

Banks that fail to take reasonable steps to detect and prevent money-laundering activity risk government fines. They also may receive severe negative publicity that harms their reputations.

Several developments over the past few years reflect the federal banking agencies' increasing concern about BSA/AML compliance efforts. For one thing, the Financial Crimes Enforcement Network (FinCEN) introduced customer due diligence (CDD) rules that require institutions to incorporate beneficial ownership identification requirements into existing CDD policies and procedures.

Within the past few years, the Office of the Comptroller of the Currency (OCC) alerted banks to increasing BSA/AML risks associated with technological developments and new product offerings in the banking industry. In addition, regulators increasingly have

been scrutinizing automated monitoring systems used by banks to detect suspicious activity to ensure that they're configured properly.

Regulators haven't limited their heightened scrutiny to larger banks. In fact, some large banks have restricted certain customers' activities or closed their accounts because of BSA/AML concerns. As a result, higher-risk customers often have moved to smaller banks with less experience managing the associated BSA/AML risks.

> DATA VISUALIZATION SOFTWARE, WHICH IS COMMONLY USED AS AN ANTIFRAUD WEAPON, EXCELS AT SPOTTING NEW OR UNKNOWN AML ACTIVITY.

HOW TO USE VISUAL ANALYTICS

Data visualization software — also known as visual analytics — can be a powerful AML tool. Traditional AML software products and methods do a good job of detecting *known* AML issues. But data visualization software, which is commonly used as an antifraud weapon, excels at spotting new or unknown AML activity.

As criminal activity becomes more sophisticated and more difficult to detect, traditional AML software or methods may no longer be enough. Data visualization software creates visual representations of data. These representations may take many different forms, from pie charts and bar graphs to scatter plots, decision trees and geospatial maps. Visualization helps banks identify suspicious patterns, relationships, trends or anomalies that are difficult to spot using traditional tools alone. It's particularly useful in identifying new or emerging risks before they do lasting damage.

Criminal enterprises that wish to launder money typically use multiple entities and multiple bank accounts, both domestic and foreign. Using data visualization software, banks can map out the flow of funds across various accounts, identifying relationships between accounts and the entities associated with them. Data visualization can reveal clusters of interrelated entities that would be difficult and time-consuming to spot using traditional methods.

These clusters or other relationships don't necessarily indicate criminal activity. But they help focus a bank's AML efforts by pinpointing suspicious activities that warrant further investigation.

USE ALL THE TOOLS AT YOUR DISPOSAL

Money-laundering is an insidious and ever-present risk, and fraudsters are increasingly technology-savvy. Your bank needs to be alert to the potential dangers and use every analytic tool available to head them off, including data visualization software mapping. ■

BANK WIRE

REGULATORS FOCUSING ON LIQUIDITY RISK MANAGEMENT

Liquidity risk is in the spotlight, given last year's notable bank failures and federal banking regulators' explanations of the underlying causes. As regulators focus on liquidity risk management, they're reminding banks that their 2010 "Interagency Policy Statement on Funding and Liquidity Risk Management (SR 10-06)" continues to be the primary guidance on the subject.

The policy statement discusses eight critical elements of sound liquidity risk management:

1. Effective corporate governance,
2. Appropriate strategies, policies, procedures, *and* limits used to manage *and* mitigate liquidity risk,
3. Comprehensive liquidity risk measurement and monitoring systems that are commensurate with the bank's complexity and business activities,
4. Active management of intraday liquidity and collateral,
5. An appropriately diverse mix of existing and potential future funding sources,
6. Adequate levels of highly liquid marketable securities free of legal, regulatory or operational impediments that can be used to meet liquidity needs in stressful situations,
7. Comprehensive contingency funding plans that sufficiently address potential adverse liquidity events and emergency cash flow requirements, and
8. Internal controls and internal audit processes sufficient to determine the adequacy of the bank's liquidity risk management process.

Banks need to follow these guidelines to ensure appropriate liquidity risk management. ■

JUNK FEES IN THE CROSSHAIRS

Federal agencies, including the Federal Trade Commission (FTC) and the Consumer Financial Protection Bureau (CFPB), are cracking down on so-called "junk fees" charged by banks and other businesses. Recently, the FTC issued a proposed "Rule on Unfair or Deceptive Fees," which would prohibit businesses from misrepresenting the total cost of goods or services by omitting mandatory fees from advertised prices and misrepresenting, or failing to disclose, the nature and purpose of fees. Although the FTC has no authority over banks, the CFPB has indicated that it will enforce the rule against violators in the financial industry. ■

WATCH OUT FOR PIG BUTCHERING SCAM

In a recent alert, the Financial Crimes Enforcement Network (FinCEN) warned banks about a dangerous virtual currency investment scam known as "pig butchering." Given the devastating impact of this scam, FinCEN has asked banks to report suspicious activities indicative of this scheme. According to FinCEN, the scam resembles "the practice of fattening a hog before slaughter." Criminals use fake identities, elaborate storylines and other techniques to convince victims they're in a trusted partnership before defrauding them of their assets.

The alert explains the scheme and provides a detailed list of behavioral, financial, *and* technical red flags to help banks identify *and* report suspicious activity. It also reminds banks of their reporting obligations under the Bank Secrecy Act and reviews the filing instructions for suspicious activity reports. ■

acxell ("acxell") has been meeting the specific risk management needs of community banks of all sizes since 1991. As a high quality and affordable alternative to other firms, acxell provides internal audit, regulatory compliance, BSA/AML, information technology, SOX/FDICIA and enterprise risk management review services and software. acxell is exclusively dedicated to the banking industry, providing clients with dedicated, focused and hand-held services reflective of a wide range of skills, experience and industry expertise. As a Firm, we have also been proactive in assisting our clients with the designing, implementation and testing of the internal control environment to assist management with the attestation requirement under the Sarbanes-Oxley Act.

acxell's uniqueness is characterized by its experienced staff and partners. Their hands-on involvement on each engagement provides our clients with a wide range of skills, experience and industry expertise. We employ the use of Subject Matter Experts — designated individuals performing audits in their specific field of expertise. The use of such professionals provides a unique value-added approach that is both efficient and productive.

We believe that a significant aspect of our services is our degree of involvement and responsibility to assist management by making suggestions for improvement, keeping them informed of professional developments and by acting as an independent counsel and sounding board on general business matters and new ideas.

We pride ourselves in our ability to provide effective and practical solutions that are commensurate with our clients' needs by emphasizing high-quality personalized service and attention. Our services are truly customized.

For **Solutions** *to your risk management needs, please contact our service coordinators at (877) 651-1700, or log-on to www.acxellrms.com to learn more.*

www.acxellrms.com

Headquarters:
646 US Highway 18
East Brunswick, NJ 08816

Offices:
New York, NY
Philadelphia, PA
Chicago, IL
Miami, FL