SAWYERS & JACOBS

The Sawyers & Jacobs Portfolio of Brands

REDTORCH CONSULTING™ REDTAIL RISK MANAGEMENT™ REDWOLF CYBERSECURITY™ REDCAPE TECH SUPPORT™

TOP TEN TRENDS
IMPACTING BANK TECHNOLOGY FOR 2024

By Jimmy Sawyers

"Look at all those chickens!" — Popular Vine Meme

Before TikTok there was Vine, and one of the more popular vine memes was of a little girl mesmerized by a flock of geese gathering around her, which led her to exclaim, "Look at all those chickens!" "Chickens" they were not, but the meme lives on and still makes me laugh every time I see it.

The meme reminded me of an old business fable about ham and egg breakfasts. ***The chicken is involved, but the pig was truly committed.*** Such is the case for bank technology ventures. A lot of eggs continue to be laid, but true commitment has been rare. As bankers crank up the due diligence requirements and regulators place renewed emphasis on third-party risk management in 2024, successful tech providers will have to show some commitment and sustainability. ***Commitment*** in the form of ownership and management having some skin in the game. ***Sustainability*** in performance and profitability for a solution that truly is in demand and solves a problem for bankers.

I'm optimistic that 2024 will be the year that true innovators make the cut and emerge as valuable solutions to help bankers compete in a market that demands world-class digital services but still values stability and trust.

To help bankers clearly distinguish the chickens from the pigs, I offer the following predictions.

PREDICTION #1

The Robots Arrive as Artificial Intelligence (AI) Gains Unstoppable Momentum

AI hits the mainstream in 2024 and promises amazing productivity gains combined with unimaginable progress, yet AI is not without risk. Unintended consequences must be considered, and risk must be mitigated and regulated, but make no mistake—AI will not be stopped.

Microsoft's multibillion dollar investment in ChatGPT maker-OpenAI will birth more than just a few nifty computer tricks and productivity gains. Already being tested as Amazon warehouse workers, expect human-like robots to be the next evolution of AI. Bipedal and wheeled robots will become commonplace for industrial and domestic use. I've had my robot dog, Astro, for almost one year. He rolls around my place and serves as an excellent guard dog when I'm away, offering me mobile live views via my iPhone. More AI capabilities will be added to Astro in the years to come, increasing his utility and my usage of his services.

As noted in my 2017 predictions ("Artificial Intelligence will be the next big thing"), AI made its way into banking via Natural Language Processing (NLP) driven by virtual assistants and voice banking years ago and is now making strides in Robotic Process Automation (RPA) and machine learning. As an early adopter of Amazon Echo (Alexa, I love you!), I've enjoyed the convenience of home automation as well as quick access to information.

In the meantime, before the robots change the world as we know it, Microsoft Copilot and Google Gemini (formerly Bard) to name two AI apps, will bring AI capabilities to the masses and become part of normal work routines.

Hardware gets a boost not seen in decades as generative AI could triple the market for servers and semiconductors. The Rabbit R1 is essentially the iPod of early AI hardware devices, showing us how AI can be incorporated into our personal lives with these Large Language Models (LLMs). However, we've just scratched the surface of AI applications in banking and in our personal lives.

Watch out for many companies engaging in "AI washing," which means a company is overstating its AI capabilities and misleading customers and investors to believe that AI is used extensively in its offerings. "I used ChatGPT to create this marketing piece" does not an AI company make.

In cybersecurity, AI presents opportunities and threats: opportunities in that AI will allow more activity to be monitored and will help banks detect malicious traffic earlier and take action to prevent or contain breaches, and threats in that hackers will use AI to launch more sophisticated and complex attacks. Data integrity will be key as bankers scrub their data so it can be used effectively in AI applications.

Ready or not—AI is here. Smart bankers will devote research dollars to learning how AI can make their banks perform at a higher level. Are robot tellers on the near horizon?

CHALLENGE QUESTION

Is Artificial Intelligence evaluation part of your bank's strategic plan?

PREDICTION #2

Microsoft's Significance in Banking Expands with New M365 Features

As more banks migrate their Microsoft applications to the cloud, we will see expansion of Microsoft 365 use as new features are added that promise to enhance employee productivity and bring Artificial Intelligence to the desktop with its new aforementioned Copilot AI offering. As Microsoft Teams has been greatly refined over the past year, we will see this tool skyrocket in usage and surpass Zoom as the videoconferencing leader.

Expect a few contrarian banks to attempt a move to Google, using the argument and buzzwords of "cloud" and "collaboration" as if Microsoft does neither and Google has the market cornered on both. Bankers should consider the pros and cons of such a risky and unorthodox move. I would not want to lose the new hot-shot commercial lender I just hired because my CIO is forcing her to use Google Sheets over Excel.

A good due diligence question for any provider is, "How do you make your money?"

Most of Google's revenue (approximately 57%) is derived from advertising. Microsoft, a more diversified company, generates its revenue from productivity and business processes, intelligent cloud services, and more personal computing, each representing about one-third of the revenue pie, with cloud services being the most profitable and fastest growing.

As with any major tech move, executive management and the board should require documented due diligence and a strong, formal written business case for the migration. Just taking the IT staff's word for it because "they know more about computers" is weak leadership.

Email, word processing, spreadsheets, calendars, chat, videoconferencing—pretty boring but critical applications for any business. Let's not introduce complexity and confusion where none should exist. Happy, productive employees plus satisfied, trusting customers are still a winning combination for profitability in banking.

CHALLENGE QUESTION

What is your bank's current utilization of Microsoft tools, and are your people trained to be proficient in the applications they use on a daily basis?

PREDICTION #3

Zombie Fintechs Lose Their Brains (Funding) and Finally Die

I'm a big supporter of innovation, and I'm an advocate of banks partnering with reputable, stable, and marketable fintechs. But the same business rules apply. One must do the proper due diligence on the front end and the proper vendor management during the relationship.

Some bank and fintech partnerships are the equivalent of letting your wife's college boyfriend live with you until his bitcoin podcast becomes profitable. The resident party might not have the host's best interest in mind.

Two indicators of the tough row that fintechs and neobanks must hoe are the planned funerals of Marcus and Mint. After acquiring GE Capital Bank's consumer deposit solution in 2016, Goldman Sachs opened its digital bank, Marcus. Approximately $4 billion in losses later, Goldman is exiting the consumer banking arena. The Marcus website is still up, but it's not offering what it originally did. Goldman is also ending its Apple Card venture. Turns

out, mere ownership of an iPhone does not constitute good credit. Imagine that! Goldman's net charge-off rate of 2.93%, compared to 0.76% at American Express, is an indicator of the subprime nature some of those loans represented. A large portion of Goldman's Marcus loan portfolio was sold at a huge loss. (Source: Fintech Blueprint, 12/4/23)

Intuit is shutting down Mint, one of the most popular Personal Financial Management (PFM) apps for consumers. While Intuit spins this as "reimagining Mint" and as part of Credit Karma, users who have poured their personal financial information into the Mint app will no longer have access as of March 24, 2024. Smart bankers learned long ago that the average consumer does not have the appetite for the accounting and discipline needed for PFM apps, a tech solution to a problem that doesn't exist nor is in demand. See my 2020 predictions on this tech time waster. Customers sign up for it, the bank pays the vendor monthly per user fees, but customers don't use it once they see the work required, and the bank gets no ROI for what is often a significant investment of time and money.

In 2024, bankers will be less fearful of being totally disrupted out of business by neobanks, most of which have produced rather anemic returns.

Varo, one of the only chartered neobanks in the US, lost one million accounts in 2023. To be fair, some were low-balance, inactive accounts (like the one I opened just to check the customer experience) and should be jettisoned. However, this could also be an indicator that starting a bank to serve people with little money to deposit and an inability to repay loans is not exactly a sound business plan for a bank.

It's hard to have a successful bank on interchange revenue alone (and that is 60% of Varo's revenue), so time will tell if Varo is the innovative bank it claims to be. For now, Varo is a well-capitalized, wildly unprofitable bank with no indication of sustainability. It continues to spend more money than it makes ($1.75 spent to generate $1.00 of revenue according to 9/30/23 FDIC efficiency ratio data).

Winning banks will leverage their traditional brands and learn they can partner with reputable and stable fintechs to do anything a neobank can do—only better!

CHALLENGE QUESTION

Does your bank require documented due diligence of new technology solutions and their providers, or does the IT staff have a blank check and carte blanche?

PREDICTION #4

Service Trumps Technology as Core Evaluations and Migrations Increase

In the many core evaluation engagements we have with banks, our clients rarely convert to another core because of technological shortcomings. The most common reason for leaving the incumbent core is not a very technical issue: it's SERVICE. Complaints about lack of responsiveness, poor support, and a revolving door of account managers are often the reasons that compel bankers to go through the pain of a core conversion. In 2024, tech providers will realize that developing new applications without considering service and support is a short-term, losing game.

As a case in point and to borrow a customer service example from another industry, I travel frequently and am often on the move, so fast food is sometimes the only option to keep me fueled. Arguably, there are a lot of places to stuff fried chicken into my mouth, but Chick-fil-A dominates its markets and remains one of my favorites because of one thing—service. When lines get long at Popeye's or KFC, I don't see well-mannered employees with iPads and credit

card readers taking my drive-thru order. Excellent service and reliable technology make for a "pleasurable" customer experience. Bankers take note. Customers don't care about the technology. It's not the chicken or the tech. It's the service, yet service is made better when the proper tech is provided to your people.

Bankers will continue to demand better service from their tech providers so bank employees, in turn, can provide better service to bank customers. One without the other is just a case of heartburn.

CHALLENGE QUESTION

When negotiating your bank's core contract, what service level agreements are in place?

PREDICTION #5

Ransomware Attacks Increase as Bankers Learn That "Cybersecurity Theater" Is Not True Risk Mitigation

As noted last year, ransomware remains the top cybersecurity threat to all organizations but especially to banks, many of which are unprepared for the reality of such an attack.

Currently, banks benefit from the fact that less regulated (and sometimes less secure) organizations, such as municipalities and healthcare, are often easier targets, but that should not cause bankers to breathe easy thinking that their banks are less vulnerable.

The new year will see too many bankers still engaged in "cybersecurity theater" as executive management relegates cybersecurity preparedness to IT staff intoxicated by too-frequent phishing testing and other "style over substance" exercises that do little to mitigate the risk of ransomware attacks.

In our work with banks, business email compromise (BEC) incidents and ransomware attacks are still the most common cybersecurity incidents that lead to major financial losses at banks. BEC risk can be greatly mitigated through simple hardening of email systems and proper testing by a qualified and independent firm.

Ransomware attack risk mitigation is more complicated and multi-layered, with the most important exercise often being the tough discussion and what-if scenario of what bank management and the board will do when hit with such an attack. If the victim bank's first calls are to a public relations firm and a government agency, expect chaos and irreparable damage to the bank's reputation and legitimate questions about management's competence to handle a crisis. Bankers must face reality and seek advice and guidance from experienced firms, preferably in advance of any incident, so that the proper scenarios can be considered, discussed, and mitigated.

Delusion is not an effective strategy when it comes to cybersecurity preparedness.

CHALLENGE QUESTION

Are your bank's cybersecurity preparedness efforts truly effective, and have they been tested by an independent and qualified firm?

PREDICTION #6

Bankers Co-Source with Trusted Experts to Complement Internal Teams

Community-based financial institutions are finding it harder each year to attract and retain IT talent. Some of these challenges can be attributed to years of outsourcing key systems and critical business functions that in the past provided training grounds for their operators and administrators. Like a major league baseball team that has a poor farm system, many bankers are not preparing rookie employees for playing in the big leagues someday, hence the talent vacuum.

Large banks can give people the opportunity to specialize in certain tech jobs, but the majority of banks (those below $1 billion in total assets) tend to develop people who are required to "wear more hats" and take on several duties. Yet, some tech employees, void of leadership and coaching, gravitate to what they want to do and not necessarily what the bank needs them to do. In recent years, this lack of clear direction has led to many "overnight" cybersecurity experts in bank IT departments who are watching screens instead of helping their fellow bank employees.

Let's face facts. If your CIO or IT manager truly were a cybersecurity expert, he or she probably wouldn't be working at your bank.

The ideal CIO in a community-based financial institution is a generalist, someone who can coordinate all the areas required to support the bank's business goals with effective application of technology and innovation. Wise CIOs develop a team of external resources, those experts who can be called upon for specific needs and special projects. It's often best to "rent" rather than "buy" such expertise.

As demands for diverse experience increase in banks due to needed expertise in cybersecurity, vendor management, strategic tech planning, network administration, risk management, and tech provider evaluation, expect bankers to assemble more external teams of trusted advisors to complement in-house players who are wearing the bank's jersey.

No one person can be expected to know it all or do it all when it comes to leading a bank's technology efforts. CIOs who try are committing career suicide. CEOs who allow it are not properly leading their banks.

CHALLENGE QUESTION

Who are the most valuable players on your bank's external tech team, and what roles do they play to help your people and your bank succeed?

PREDICTION #7

Innovation Comes to Lending

It seems to make perfect sense to devote tech budget dollars to the business function that generates most of the bank's revenue; however, banks continue to throw money at technology solutions to problems that don't exist (read: PFM applications) while neglecting the lending area.

Expect lending to take center stage in 2024 as bankers work to coalesce all the current, fragmented lending solutions into a contiguous, integrated process that yields impressive returns.

Lending tech islands of decisioning, spread analysis, documentation, workflow, relationship management and money movement will be connected to bring long-awaited harmony to this critical function. Expect some of the new successful fintechs to be acquired by major traditional players to provide the bridge to this innovation. Banker scrutiny and proper vetting of lending solutions and their providers will balance the market and expose those who have over-hyped their offerings.

Leveraging AI in lending could really blast banks into a whole new world.

Is your lending function a cobbled-together mess of disparate systems that confuse and frustrate, or is it a streamlined process that customers love and lenders leverage? Few if any banks have a completely integrated lending process. Most banks must still depend on many systems to make a loan. However, innovators are working to fuse the lending function with new systems and better business processes.

CHALLENGE QUESTION

From application to servicing, is your lending process operating as desired?

PREDICTION #8

Banking as a Service (BaaS) Tanks as Regulators Finally Step in and Step up to Protect Bankers from Themselves

The chickens let the fox into the henhouse and are now surprised the fox is broke and not paying rent on time. More disturbing, the fox has also introduced risk (e.g., Bank Secrecy Act issues) to the formerly peaceful and profitable farm, and the chickens now wish they had performed more due diligence before engaging Mr. Fox.

Such is the case with some Banking as a Service (BaaS) relationships where bankers, often inspired by a shill on stage at a conference at a nice resort, have invited the very people who want them out of business into their traditional banks where they are now providing core and debit card processing services to what could be classified as fake, largely unregulated banks.

Despite helping some core providers and consultants increase revenues, the BaaS experiment has brought regulatory enforcement to some of the banking leaders in this niche. According to S&P Global Market Intelligence, BaaS banks accounted for 13.5% of all severe enforcement actions issued to US banks in 2023.

If you've read my predictions from previous years, been in my banking school classes, or heard me speak at conferences, you know I've advanced a few unpopular opinions on the blind trust many bankers have put in fintechs as well as the "drink the Kool-Aid" mentality of some who get persuaded to provide core and debit card processing services for the very fintechs and neobanks that are vying for their market share. Sadly, independent and objective advice is rare these days, and even rarer is the ability for some to distinguish the charlatans from the trusted advisors.

By the way, Banking as a Service is nothing new. Most community banks were processed by their correspondent banks back in the 1970s and 1980s, but the advent of midrange computers and later client-server-based systems helped these community banks cut the cord of dependence from their large-bank brethren and usher in a new era of innovation of nimble operations.

"A swift kick in the BaaS" fad will help stabilize the banking industry and reward traditional community bankers who have the wisdom to focus on tech solutions for their bank, its customers, and their communities—not the parasitic companies that bring unnecessary and unprofitable risk.

CHALLENGE QUESTION

Are you leveraging your bank's reputation of trust and high performance to innovate and improve the customer experience and profitability, or is your focus on providing processing services for companies trying to put you out of business?

PREDICTION #9

Risk-Tech Management Gets Redefined

Banking isn't getting any less risky, hence the need for effective risk management at all levels. As innovation outpaces regulation, we are now seeing regulators catch up to the market and lower the hammer on certain areas, notably third-party risk management and cybersecurity.

Many bank-fintech partnerships are mutually beneficial and help both parties succeed. In these cases, there has typically been proper due diligence performed by the bank, a strong, formal contract (drafted by a qualified attorney) between the two parties, and measurable performance by the fintech. Vet-contract-perform (VCP). These fintechs tend to have good leadership with a healthy work ethic, not just a parasite with a get-rich-quick mentality.

Third-party risk management (i.e., vendor management) is only one part of a bank's overall risk management program, but it is an increasingly important part these days. Expect bankers to step back and review all risk management functions for effectiveness, from risk assessment models to business processes. The time has come to apply innovation and critical thinking to risk management.

I remain bullish on bank-fintech partnerships that follow the VCP formula. In 2024, expect bankers to get more formal when entering into such agreements. Otherwise, to paraphrase Benjamin Franklin, houseguests, like fish, begin to stink after a period of unprofitability, underperformance, and broken promises.

CHALLENGE QUESTION

Have you taken a fresh and holistic look at your risk management programs to determine if they are truly creating awareness and mitigating risk to an acceptable level?

PREDICTION #10

Strategic Technology Planning Becomes More Critical as Finite Resources Force Bankers to Pick Their Battles

Today's tech choices can be overwhelming. Follow the herd or break away? Listen to biased sources who are salespeople-in-disguise or seek independent advice? Risk your bank's reputation by choosing the wrong solution?

Sorting the players from the pretenders is not getting easier. Assessing your bank's past and current tech performance as you chart a path to the future by defining where you want to go and how you get there is a valuable exercise that brings focus to complex decisions.

Many bankers have not gone through a strategic technology planning exercise post-pandemic, but it's time they did so. To be competitive in a world that is forever changed by digital apps that allow us to order groceries, request a car ride, or have dinner delivered, bankers must listen to their customers and their employees to map out a tech strategy that keeps their banks relevant.

CHALLENGE QUESTION

Does your bank have a formal strategic technology plan that keeps your team focused and moving forward?

SUMMARY

Sir Arthur Ignatius Conan Doyle, creator of the character Sherlock Holmes, said it best: "Once you eliminate the impossible, whatever remains, no matter how improbable, must be the truth." In 2024, bankers will find truth in technology as the "impossible" is eliminated through due diligence and continued innovation for tech providers who are committed to helping bankers improve the customer experience, employee productivity, and risk management. Take care of those three areas and profitability and high performance, along with that other important factor—truth—follows.

Here's to a new year full of innovation and mutually beneficial bank technology provider relationships.

Jimmy Sawyers is Co-Founder and Chairman of Sawyers & Jacobs LLC,
and is one of the most independent and informed voices in the industry. Leaders in Innovation-Risk Management-Cybersecurity-Technology through the firm's four brands.

SAWYERS & JACOBS

The Sawyers & Jacobs Portfolio of Brands

REDTORCH CONSULTING™ REDTAIL RISK MANAGEMENT™ REDWOLF CYBERSECURITY™ REDCAPE TECH SUPPORT™

REDTORCH CONSULTING:

LIGHTING THE PATH TO HIGH PERFORMANCE

Strategic consulting designed to align people, processes, and technology for world-class innovation, management, and operations.

REDTAIL RISK MANAGEMENT:

WATCH RISK LIKE A HAWK

A suite of risk management services designed to help bankers identify threats and mitigate risk through practical applications, comply with laws and regulations, and maintain a high level of customer service, security, and profitability.

REDWOLF CYBERSECURITY:

PROTECT THE PACK

A full range of cybersecurity services for those serious about securing the enterprise and repelling the attackers who threaten the bank and its customers.

REDCAPE TECH SUPPORT:

YOUR HERO IN TECH

Concierge-level tech support delivered in a strong, intelligent, and friendly manner with premium quality, superior service, and special attention.

For more information, visit sawyersjacobs.com, call 901.853.1000, or email jsawyers@sawyersjacobs.com.