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 2023

By Jimmy Sawyers

"The folly of mistaking a paradox for a discovery, a metaphor for a proof, a torrent of verbiage for a spring of capital truths, and oneself for an oracle, is inborn in us."

— Paul Valéry

Oh, how we want to believe! We are, by nature, an optimistic and trusting species. The speaker on stage at the banking conference must be vetted and legitimate or the association wouldn't have put that person on the agenda. The author of the article in the banking magazine must be independent and provide information for the greater good of the industry. That guy who runs that cryptocurrency exchange has to be a genius. That cybercriminal now turned consultant must now have a heart of gold and a spirit of service. We want to believe the best...so much so that our good judgement is often clouded and we fail to notice the red flags, the half-truths, the lack of proof and performance. We rise to the bait and only with the benefit of hindsight do we realize we have been defrauded and that we should have performed more due diligence.

As Valéry noted, this folly exists in all of us. We often overestimate our powers of prophecy. Yet, we all reach a point where the tolerance for talk is replaced by a requirement for action...for performance...for delivering on the promises of yesterday by providing value today.

Such will be the case in 2023 as bankers, weary from years of promises made by tech startups, will require proof before signing contracts and making tech purchases based on faith and folly. ***To that end, I offer my ten predictions that I hope will steer you on the right path to success and sustainability in your bank's future.***

PREDICTION 1

Fintechs Face a Year of Reckoning

2023 will be the year of reckoning for fintechs as the cost of capital increases and bankers demand results. Many fintechs have enjoyed the easy money of the last decade to buy customers and marketing in hopes they can grow their way to profitability. Most failed. Fundamental business rules were ignored. When the cost of funds was zero, any fool could appear legitimate. Now we will see which fintech players have real business models and which ones were just playing with other people's money (or defrauding investors).

One example: JPMorgan Chase bought the student loan/financial aid fintech, Frank, for $175 million. According to a lawsuit filed earlier this year by JPMC, the owners of Frank overstated their number of accounts. When JPMC emailed the borrowers, 70% of those emails bounced back. It is now believed that Frank may have had nearly four million fake accounts.

Based on a January 11, 2023, article in Forbes, the founder of Frank, 30-year-old Charlie Javice, created a roster of 4.265 million fake customers. These "students" did not exist. The lawsuit estimates that Frank only had approximately 300,000 customer accounts, but even that number should be questioned.

Due diligence remains critical. When JPMorgan Chase gets duped, even with their vast resources, anyone can.

CHALLENGE QUESTION

Does your bank have a fintech relationship that has changed your bank for the better, or have performance and ROI been non-existent?

PREDICTION 2

Crypto Bros Punch One-Way Tickets to Hell

In my opinion, Bitcoin is the biggest lie told in the history of payments and tech. It remains an asset class to be traded and a mechanism to avoid the rule of law and taxation. Despite the hype, it is not used in normal, everyday transactions. Actually, I'm not sure we can call it an asset class any longer. Crypto in general is an unregulated and rigged system.

Google "FTX" and "SBF" on your own time. Enough said.

How does crypto fraud affect banks? Take the fintech Dave, for example. Turns out Dave received a $100 million loan/investment from FTX. According to a CNBC article (December 28, 2022), Dave has a $101.6 million liability to FTX. Further, the article notes that the loan/investment to Dave was made with FTX customer deposits. Dave gets its core processing from a traditional bank. The degrees of separation are few. Stay tuned to see how this pans out.

Silvergate Bank, a pioneer in supporting fintechs and cryptocurrency innovators, recently discontinued its crypto payments network, the Silvergate Exchange Network, and warned investors that losses could result in the bank being "less than well capitalized."

Put your money in unregulated exchanges at your own risk. The "smartest guys in the room" are being exposed for the charlatans they are.

The silver lining here will be a new influx of deposits to banks as trusted providers in a rising interest rate environment. Wise bankers will be ready to facilitate that exchange with a strong suite of digital services.

CHALLENGE QUESTION

How much time and money has your bank spent courting crypto, a movement that wants you to no longer exist?

PREDICTION 3

Artificial Intelligence Attracts Investment

As interest wanes in Web3 and cryptocurrency, we will see increased interest in Artificial Intelligence (AI) with investments shifting to AI projects. The question remains…how will these companies become profitable? What problems will AI solve? Do we have the quality data to effectively deploy AI, as AI must have good data before it can be effective? Will ChatGPT replace our loan officers?

This will be the year when bankers seek answers to these questions in hopes that AI technology will deliver on the promise of more efficient operations and increased automation of, at a minimum, the most mundane tasks of banking.

CHALLENGE QUESTION

What is your AI strategy, and how can it be applied in your bank?

PREDICTION 4

Bankers Get Digital (and Physical)

As of December 2022, FDIC data shows we had 30,684 more banking locations than we had in 1987, despite a shrinkage of 9,651 commercial bank charters in the period. Surprised? The branch is still an important channel.

While these physical locations are transforming, they remain important strategic assets for bankers who implement world-class digital services, some of which might be accessible in the branch lobby.

Expect to see more Interactive Teller Machines (ITMs), sans the video teller component, move from the drive-thru lane into the branch lobby to reduce staffing and to facilitate self-service. This "human plus machine" strategy will be a winner for most banks.

CHALLENGE QUESTION

What is your bank's branch tech strategy?

PREDICTION 5

Hybrid Work Environments Drive Demand for Tech

"Quiet quitting" became "loud layoffs" in some sectors as big tech trimmed payrolls. Expect more of the same in 2023 as we see a return to the meritocracy where high-performing employees are rewarded and low performers are jettisoned. Visibility matters in any organization but especially in banking, a people-focused relationship business.

In some cases, white collar jobs have become no collar jobs as some want to sit at home in their sweats and pet their cats instead of heading to the office and performing collaborative work in a more suitable environment. These no-shows are often the first people laid off during downturns.

Of course, there are exceptions, and some jobs are well suited for remote work. However, 2023 will bring some back to reality as managers realize that productivity, teamwork, and culture can suffer if all work is remote.

As someone who has spent most of his career working from bank boardrooms and hotel rooms, I know mobile workers can be highly productive if given the right tech tools without unnecessary restrictions and ill-advised controls (e.g., requiring VPN access to simply access work email).

Expect hybrid work environments where people are given more flexibility to work from home with prudent parameters to drive demand for tech to support this mobile workforce.

CHALLENGE QUESTION

Does your bank have the right technology and security in place, properly configured, to support remote work?

PREDICTION 6

The Core Market Shrinks as New Cores Continue to Be Bores and Old Cores Are Sunset in Record Numbers

As our firm helps banks across the nation evaluate core providers, two trends have become evident. One, the promise of new cores fully replacing legacy cores has been greatly oversold, and two, legacy cores, many of which have been starved of new investments for years, will finally be taken out behind the barn, Old Yeller-style, and put out their misery…sunset, discontinued, gone.

In a shrinking market of bank charters, core providers must become more efficient by reducing the number of solutions they support. This will create some market movement as many bankers say, "If I have to convert anyway, I might as well see what else is out there." Expect a wave of core provider evaluations and more conversion activity than we've seen since the late '90s when Y2K and new client-server based systems drove many core migrations.

New cores have failed to reach any critical mass necessary to be considered viable solutions. Most remain niche players with limited features, the equivalent of going to The Home Depot to buy lumber and nails to build your own house, more parts than turnkey solutions…a Frankenstein's monster that must be bolted together. Most bankers don't have the appetite or the budget to build an expensive core from scratch that does the same thing as

the old core. Expect to see some of these solutions acquired by traditional providers and absorbed into current core solutions as add-on features and ancillary systems.

Smart bankers will pull out their core contracts to see if "sunset clauses" exist and determine whether their core migration path decision has been made for them contractually by the provider, or if they have time to evaluate other solutions. Those who ignore this inevitable event will find themselves boxed into a core solution they might not want at a price they don't want to pay, hence the need for proper due diligence and intelligent evaluation.

We tell our kids, "Show me your friends and I'll show you your future." I tell bankers, "Show me your core and I'll show you your bank's future." Assess and evaluate your core strategy now lest your future be controlled by your current core provider who may be struggling to figure out what to do with partial core solutions they've acquired.

CHALLENGE QUESTION

What is your bank's core strategy, and is your contract up for renewal within the next two years?

PREDICTION 7

Risk Awareness Drives Demand for More Practical Risk Assessment Models

Why do banks have so many risk assessments? One word. *Awareness*.

Yes, many are regulatory-driven, but the numerous risk assessments in banks, from GLBA information security risk assessments to those addressing enterprise risk or cybersecurity risk, all accomplish one common goal: to create awareness of risk and document how the bank is mitigating such risk to an acceptable level.

Banking is not getting less risky with the growing number of cybersecurity threats, vendor management woes, and an economic and political environment that presents great uncertainty.

The amount of time bankers spend on risk assessments is significant and doesn't appear to be subsiding. Like weeds in a garden, some banks' risk assessments have expanded in unnecessary complexity and now require an inordinate amount of time to complete. Plus, some models yield shaky results and cannot be easily understood by bank management or the board of directors. Now is the time to take a long, hard look at all the risk assessments your bank is completing on an annual basis and determine which ones need updating or should be discontinued.

CHALLENGE QUESTION

When was the last time you inventoried and assessed your bank's risk assessment models for applicability, relevance, and effectiveness?

PREDICTION 8

BIMOs Get Regulated and Educated

BIMOs (Banks in Marketing Only) continue to operate with impunity, free of any real regulation and allowed by federal authorities to market themselves as legitimate banks when they are not. Often the written disclaimer of BIMO TV ads that they are "not a bank" is obfuscated in tiny font, white text on a white background, while the actors in the commercial use the words "bank" or "banking" to imply this commercial is for a true FDIC-insured bank when it's really for a technology company. Where are the regulators and politicians when we need them?

From predatory lenders to these BIMOs, any entity that operates like a bank should be subject to the same laws and regulations of traditional banks. To do otherwise threatens consumers and degrades the banking industry and damages trust. Further, bank lobbyists are failing their clients as they are selectively outraged at credit unions but indifferent to fake banks.

In 2023, bankers will wake up to the fact that these BIMOs should be regulated, and their customers should be educated about their so-called "banking relationship." Again, the rising cost of capital combined with increased regulatory requirements will end most BIMOs and accrue to the benefit of traditional banks ready to receive this runoff.

CHALLENGE QUESTION

What is your competitive response to BIMOs?

PREDICTION 9

Efficiency Remains an Elusive Concept for Digital-Only Banks

I have long advocated that "digital-too" banks have a distinct competitive advantage over "digital-only" banks. Traditional banks that leverage digital services to round out their service offerings can beat digital banks at their own game if they can get out of their own way and adopt new, streamlined business processes.

To sample a few digital banks, I reached out to our friends at Seifried & Brew and Velligan-Blaxall Consultants where Mr. Jamie Sumner, Partner, noted that Varo Bank has an efficiency ratio of 324.69 percent, which means this bank is spending $3.24 to generate $1.00 in revenue—not exactly a sustainable business model. Quontic Bank sports a 214.71 percent efficiency ratio. SoFi Bank, often held up as a model for digital banks, clocks in with an 81.13 percent efficiency ratio. The community bank median efficiency ratio is 65.00 percent. High-performing community banks do much better than 65.00 percent, and most offer the same services as digital-only banks.

Sumner notes that digital banks tend to have a higher cost of interest-bearing deposits, something that does not bode well for them in a rising interest rate environment.

In banking, as in any service business, the business process is more important than technology. Do you really care how your pizza is made, or do you just want it hot, tasty, and fast? Many consumers want their banking like their pizza. They don't care what oven you used or about the POS system that took your payment. They want their banking to be as easy as ordering a pizza, whether over the phone, via an app, or in person.

CHALLENGE QUESTION

How are you changing your business processes to compete with digital banks?

PREDICTION 10

Ransomware Will Remain the Top Cybersecurity Threat

Bank CEOs often ask me what should be keeping them awake at night. Cybersecurity threats, specifically ransomware attacks, is my answer.

According to a 2022 study by CyberProof, the top two countries of origin for cyberattacks were China (18.83%) and the United States (17.05%), respectively. Many bankers have been conditioned to believe all cyberattacks come from Russia, which in this study came in at number eight behind Thailand. Even Russian cyberattacks on Ukraine have proven more damaging psychologically than financially.

In our work with banks, we continue to see business email compromise (BEC) incidents aimed at executing fraudulent wire transfers (the most recent originating in Nigeria), but every banker should be keenly aware of the ransomware threat and consider this scenario in a cybersecurity incident tabletop test. Do you have cybersecurity insurance coverage that covers ransomware attacks and potential ransom payments? Will you pay the ransom or not? How long would it take you to rebuild your network if you don't pay? There are many other questions to answer in this area.

Try to avoid the sanctimonious and high-and-mighty refrain that you would never pay a ransom. We have this tough conversation with our clients and their directors often. Like many things in life, it's easy to say what we would do until it happens to us. Be realistic and pragmatic so that you can plan ahead and be prepared.

CHALLENGE QUESTION

What is your bank doing to mitigate the risk of a ransomware attack, and what would you do if your bank suffered an attack?

SUMMARY

Fintechs will continue to push bankers to innovate and rethink traditional business processes. However, blind faith in fintech promises will be replaced by extensive due diligence and the requirement of proof. The survivors will be prepared to provide the documented proof necessary to show bankers the value of their solutions and the utility these solutions present to improve efficiency and the customer experience.

New technology must have value. It must help bankers save time and money, generate new lines of revenue, or improve the customer experience. The technology must be more than just cool. It must deliver. It must have a business case and fulfill a need. As Thomas Edison said, "Anything that won't sell, I don't want to invent. Its sale is proof of utility, and utility is success."

Here's to a 2023 filled with bank tech purchases that bring utility, success, and promote profitability based on proof instead of false prophets.

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.

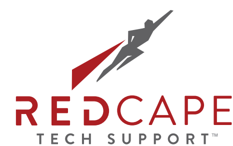
RedTorch Consulting: Lighting the Path to High Performance *- Strategic consulting designed to align people, processes, and technology for world-class innovation, management, and operations.*

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.*

The Sawyers & Jacobs Portfolio of Brands



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