SAWYERS & JACOBS

Innovation. Risk Management. Cybersecurity. Technology.

TOP TEN TRENDS

IMPACTING BANK TECHNOLOGY FOR 2020

JIMMY SAWYERS

Sawyers & Jacobs LLC

Competition whose motive is merely to compete, to drive some other fellow out, never carries very far. The competitor to be feared is one who never bothers about you at all, but goes on making his own business better all the time.

- Henry Ford

REDTORCH CONSULTING

Lighting the Path to High Performance

REDTAIL RISK MANAGEMENT

Watch risk like a hawk.

REDWOLF CYBERSECURITY

Protect the pack.

REDCAPE TECH SUPPORT

Your hero in tech.

History is full of tech that ebbed and flowed until the right formula was found. Will we ever have significant adoption of self-driving automobiles? Or, will we have pods being propelled along on some type of track system? Which solution is safer and more efficient? It's the escalator question. Should the stairs move? Should you move? Should both move? Design and workflow questions one should ask before launching any new tech.

Any soapy-handed traveler in an airport bathroom, hopping from one electric-eye sink to another as the water won't flow (or stops flowing due to a timer) knows that tech can sometimes complicate and frustrate the user experience if not designed and operated properly. If the goal is 100% automation instead of 100% customer satisfaction, new digital services will often fail.

With an optimistic outlook for focused bankers who make their businesses better and go forth with confidence and sound strategy, I offer these predictions for 2020:

PREDICTION #1

Tap-to-Pay Improves the Customer Experience and Increases Interchange Revenue

At a recent client bank board retreat in the Midwest, I was speaking to the bank's directorate on digital services strategies. One of the board members who owns several QSRs (quick-service restaurants) in airports and shopping malls was lamenting the slowness of the EMV customer experience and he was looking forward to the benefits I was touting for tap-to-pay (TTP) and related improvements in payments speed. He estimated that his customer POS transactions would go from five seconds (EMV) to one second (TTP) when customers can tap their cards instead of inserting them. That translates to real dollars when one is trying to get customers through the queue as fast as possible.

The good news for this business owner is that 63% of face-to-face transactions in the U.S. now occur at contactless-enabled merchants. Further good news is the survey that indicates debit cards are tapped at a higher rate than credit cards (4.9% to 2.8%, respectively).

As cash is used for 1/3 of such transactions in the U.S., this presents a $2 trillion opportunity for bankers who aggressively promote debit card usage, issue TTP-enabled cards, and design their systems to manage fraud risk but not be an impediment to authorized customers using this new payment method with ease. Sources: AYTM (Ask Your Target Market) Survey on Contactless, March 2017 2. NilsonReport / Euromonitor Data, Q1 17, Visa

> CHALLENGE QUESTION
>
> ***Is your bank prepared to introduce tap-to-pay to your customers?***

PREDICTION #2

Contact Centers Take on Greater Importance and Empower Agents with Decision-Making Ability Driven by Advanced Data Analytics

While the telephone may be the oldest and most unappreciated technology in banks, contact centers will be re-engineered to leverage the many communications methods available to consumers and businesses and allow customers to be served quickly, via a variety of channels, and without being transferred from department to department,.

Agents will be empowered to make decisions at the point-of-service, wowing customers in the process. Advanced data analytics will provide the information necessary to increase customer responsiveness. Need that mobile deposit limit increased? Done! Need a higher POS limit? You got it! Such decisions do not require supervisory approval if the agents are given the criteria for such decisions and the tech and system access to make it happen.

I predict banks will replace current live-chat apps with SMS text messaging apps to communicate with customers on the channel of their choice. Any parents of teenagers who have texted their kids in the next room understand that texting is easy, reliable, and normally gets a quicker response compared to other methods. Trust me. Bank employees are already texting with customers, whether bank management endorses and supports it or not. SMS text messaging solutions that archive conversations and better organize use of this handy medium will gain traction in 2020 and improve inbound and outbound customer communications in bank contact centers. This will prove a major differentiator between traditional banks and their startup competition that rarely offers such easy and personal communication.

> CHALLENGE QUESTION
>
> ***Is your bank's contact center equipped with the right tech and access, and are your employees empowered to make decisions and "wow" customers at this point-of-service?***

PREDICTION #3

Bank CEOs Assume a More Vocal Tech Leadership Role

Bank CEOs, repeat after me. I vow to never start another sentence by saying, "I don't know anything about IT so…" Would you rather know IT or banking? IT is the tool that makes efficient banking possible. IT is a means to an end. It's not banking. Bank CEOs will exert their leadership and remind IT management and staff that a bank is a for-profit institution that manages a risk-reward proposition. Shape tech to the bank. Don't shape the bank to tech.

CEOs will also take a more direct role in who the bank engages for tech advice and will look to reliable and trusted advisors who are independent of selling software or promoting fintechs. "How do you make your money?" will be the first question in the vetting.

These CEOs will also take charge of cybersecurity preparedness and give the boot to charlatans from incompetent firms posing as cybersecurity practitioners. Practical cybersecurity testing, sound risk assessments, and targeted education will replace the hyperbole of amateurs.

More documented due diligence will be performed and more scrutiny will be placed on selecting technology services providers too. Sound business questions will be asked to truly assess providers, their solutions, and their value to the bank. The old saying, "Beware the naked man who offers you the shirt off his back," will ring true as bankers scrutinize those companies that are bleeding cash and are in danger of failing.

> CHALLENGE QUESTION
>
> ***Is your bank's CEO a passive and apathetic participant in the bank's tech strategy, or does he or she take an active and energetic role in this important arena?***

PREDICTION #4

Smart Bankers Decide Doomsday Prepping is Not a Profitable Business

Overcompliance and misguided security measures are killing community banks' ability to compete. Some banks' cybersecurity programs have no basis in reality, highlighting outlandish and unlikely fears that are sucking valuable resources from profitability and productivity. Successful banks must strike the right balance to compete yet remain secure.

If IT management is locking the bank down so tightly that no one wants to work there and customers don't want to do business with you, we have a severe overreach. Often such misguided efforts result from an IT manager attending a conference, getting bad advice from a speaker who paid to be on stage, coming back to the bank and acting on that bad advice resulting in the added expense and inefficiency of an unnecessary control or superfluous solution…often purchased from…you guessed it…that same speaker.

Ideally, banking industry associations will start disclosing which speakers paid to speak (like advertisements on news sites are labeled with a dollar sign) versus which speakers are being paid for their independence, objectivity, knowledge, and expertise, so unsuspecting bankers understand they are being solicited by the former. Until that day, banker beware. Free advice is often worth exactly what one pays for it.

Spider holes are not a branching strategy. In 2020, smart bankers will cease the doomsday prepping in favor of more intelligent risk management that employs sophisticated approaches to today's complex cybersecurity threats. This will start with a major review of current risk management efforts that may be dated or off-target. Finite resources will be applied where they have the most impact and return on investment.

> CHALLENGE QUESTION
>
> ***Is your bank striking the right balance of security and convenience, or are you hearing complaints from employees and customers that business is being impeded from rigidity bordering on stupidity?***

PREDICTION #5

Traditional Banks Build a Digital Moat Around Their Castles to Repel the Invaders

As noted in my predictions last year, the so-called "open banking" being legislated in Europe and Australia is a threat to capitalism and our American banking system, in my opinion. Please don't confuse an Application Program Interface (API) for open banking. The nomenclature is being miscommunicated by those with an agenda to fast-track their fintechs up the wazoo of traditional banks.

JP Morgan Chase recently started banning third-party fintech apps from accessing customer passwords. Security concerns might be the reason given to the public, but competition is clearly the impetus for such barriers.

PNC Bank clients have complained about being unable to connect their accounts to Venmo at the Pittsburgh-based bank. In a series of tweets, PNC suggested to these clients that they "explore alternate means of money movements" such as PNC-backed P2P payment solutions. Expect banks of all sizes to stop the fintech dance and make such "money moves."

If one allows unauthorized third parties to access customer accounts, don't bemoan the fact that Mr. Fox ate your chickens. You let Mr. Fox in the henhouse. Unaware or naive bankers will reap what they have sown. Wise bankers will protect their franchises from such interlopers by constructing "digital moats" to prevent such access. Bankers have the "hammer." They no longer need to be the "nail" for third parties creeping into their proprietary and private systems.

Expect increased use of tokenization and other measures designed to gatekeep the covert scrapers yet allow trusted partners narrow and secured access with proper legal agreements in place.

Unlike Europe and Australia, there is no such open banking legislation in the United States and let's hope none is introduced. Are you listening, bank lobbyists? Get on it!

> CHALLENGE QUESTION
>
> ***How are you protecting your franchise from freeloaders, invaders, and digital squatters?***

PREDICTION #6

Business Processes Are Examined for Self-Inflicted Wounds

In our practice, we often work with new client banks that have long blamed current shortcomings on technology when the real culprit is a business process from 1995 and middle management that does not understand the risk-reward proposition that is the foundation of banking. "Can't we buy technology to fix this?" is often the refrain. The best and newest tech cannot overcome archaic business processes and bad management.

For this reason, bankers will engage qualified consultants to review their banks' people, processes, and technology to assess whether all are aligned for peak performance. Often, calibration is better than innovation.

Further improving the marriage of process and tech, increased use of facial recognition in branches, at ATMs, and at POS terminals will soon make it seem ancient to enter a PIN at an ATM or insert a card. We will pay with two things that are never far apart, our faces and our phones, the latter often serving as the second factor of authentication.

For now, I'd be satisfied with a more Square-like experience in the form of emailed teller receipts. Bankers, if Sears can email me a receipt and your bank cannot, we have a problem.

> CHALLENGE QUESTION
>
> ***Are your bank's people, processes, and technology working in harmony?***

PREDICTION #7

Twenty Years of Tech Compliance Gets Revisited and Revamped

Much of the regulatory guidance for IT is getting a bit stale and perhaps should have an expiration date. Worried about those weblinks that might take a bank website visitor to your bank's Facebook page…that you manage? The horrors! Better give that person an annoying warning in the form of a pop-up. That regulatory issuance (FDIC FIL-30-2003) came out in the early part of this century (2003) when social media was largely non-existent (Facebook arrived in 2004) but the sale of uninsured investment products to confused and misled customers was the concern.

What if your bank's website is not ADA compliant? Will the regulators shut you down? Not likely. I don't believe the current administration and the U.S. Department of Justice will come down hard on bankers with non-ADA compliant information-only websites. These worries were prompted by litigious trolls seeking an easy payday (read extortion) from scared bankers.

It's time that bankers, regulators, practitioners, and industry associations come together to review the laws, regulations, and guidelines for technology that simply may not make sense any longer or need updating. Too many finite bank resources are being drained for items that do not present any significant threats while the likely and most impactful threats are not getting the attention they deserve (e.g., ransomware and related cybersecurity concerns).

> CHALLENGE QUESTION
>
> ***In what areas are you over-complying or allocating resources to trivial risk?***

PREDICTION #8

Tech Time Wasters and Resource Hogs Are Eliminated

In my travels across this great nation helping banks, I've identified three time-wasters that are sucking resources that could be applied to more critical projects involving digital services and the customer experience.

One of these major time-wasters is automated vendor management systems that require significant care and feeding and produce little value in return. Most bankers filling these bloated systems on a daily basis are neither helping manage vendors nor making the bank more compliant. Often, we see an FTE dedicated to this daily exercise of shuffling contracts and harassing providers for often unnecessary documentation (i.e., your law firm probably won't give you its financials).

The second time waster? PFM applications. Consumers appear to be rejecting such systems. According to Raddon Research Insights, 83% of the consumers surveyed have never used a PFM app. Of the 17% who currently use or have used a PFM, 68% use an Intuit solution (Quicken or Mint). Of the consumers surveyed who no longer use a PFM app, 35% said, "I did not see value in keeping up with this program." At a recent banking industry forum I was leading, I asked for those bankers in the audience whose banks had a PFM solution to all at once give me a thumbs up or thumbs down on the solution, its performance, and its acceptance by customers. Unanimously and in unison, all thumbs went down. All of this said to say, I'm not high on PFMs succeeding in the average community bank. Invest in such solutions at your own risk and lower your expectations of customer adoption. Be careful your bank is not paying for PFM app downloads that do not have active users.

Thirdly, P2P payment solutions are still in the embryonic stage and some won't survive. Any P2P payment solution that does not ride a trusted network (e.g., debit card rails or ACH network/Fed) will fail by 2023. Current P2P payment solutions developed by large banks will be disrupted before they can gain the critical mass (i.e., number of banks enrolled and active…not the misleading metric of transaction dollar volumes) necessary to sustain a business. There is simply too much good competition that has customer loyalty for such limited, private network solutions to succeed.

Will FedNow be that disruptor? Not if it doesn't come out until 2024. Time will tell but I believe core providers will be driven by their community bank customers to offer this simple payments solution as an alternative to Venmo and SquareCash, to name two popular P2P payment apps.

In sum, check your bank for time wasters and resource hogs, and objectively assess their true value. Feed the thoroughbred, not the mouse. The former will get one around the track the fastest and into the winner's circle.

> CHALLENGE QUESTION
>
> ***What are your bank's time wasters and, as management, what are you doing to eliminate them?***

PREDICTION #9

Digital-Only Banks Get Crushed by Digital-Too Banks

In the previous year, I was often asked by bank CEOs if their (sometimes 100+ year old) banks should open a separate digital-only bank. My question to the question was often, "Did you open an internet-only bank at the turn of the century"? If not, why not? And, if not, why would 2020 be any different than 2000?" Now, certainly we're in a different age due mostly to the advent of the smartphone and the advances in the networks that bring them utility. However, some of the same business cases apply.

Instead of a digital-only mindset that risks making a successful bank franchise just like its larger competitors and startup challengers, I encourage these bankers to leverage their differentiating attributes and follow a "digital-too" strategy. These banks can do anything a fintech can do by building their own solutions, partnering with trusted and stable startups, or cajoling their core providers to acquire or build new applications.

I don't believe in scrapping what made a bank great for over 100 years just in the name of digital. New digital services are often 80% complementary and 20% disruptive. Such is the case with banking. Don't try to be a fintech. Just be a better bank.

> CHALLENGE QUESTION
>
> ***Is your bank experiencing digital angst or does it have a digital services strategic plan?***

PREDICTION #10

New, Lightweight Cores Will Flip, Flop, and Die…not Fly

To paraphrase the old Johnny Lee song, some bankers are looking for core love in all the wrong places.

I remain highly skeptical of anyone claiming to have a new core banking solution that will revolutionize banking as we know it.

Why? First, who in his right mind would write a new core banking software solution in a rapidly shrinking market of banks? Take that business plan to Shark Tank and one would not last long.

"Hello, Sharks! I'm Jimmy from Memphis and I've developed a new software for a market of less than 5,000 customers who rarely leave their current solution which, on average, they have used for 15 years or more, are typically under contract for five years at least, and abhor conversions (read change). The sales process typically takes one year and then it takes at least another year to convert. My competitors are proven, established, and normally have loyal customer bases (due partly to years of good performance but also due to some bodacious user conferences). Our marketing plan is to use so many buzzwords that bankers buy our solution just because it sounds good. We don't want to respond to any real RFPs because we won't put our claims in writing (on the advice of our legal counsel). I've invested millions of dollars to write this code and I'm going to give you the opportunity to invest in my company. So, tell me Sharks, are you ready to post some debits and credits and accrue some interest"?

The evisceration would be swift. Good TV. Bad business pitch.

Is it a bad thing that traditional cores are stable, reliable, and get the job done daily in a boring, dependable fashion? There is a reason I have two different people/firms for my taxes versus my marketing. I want my CPA to be conservative and stable. I want my marketing guy to be creative and edgy. I don't expect them to wear the same clothes or attend the same parties. They are different for a reason and that is a good thing in my book.

The stability of current core systems should not be discounted. Both Chime and Venmo have experienced significant outages recently. I can't think of one of my community bank clients that has had the same issues, especially those that remain on-premise with their cores and control their business continuity/disaster recovery preparedness.

While I wish a new, robust, and ready-for-prime time core banking solution would be developed, I'm not optimistic and, much like Sasquatch and the Chupacabra, I've not seen a viable one yet in the wild or in captivity, but I've heard the tales.

For this reason, I predict that bankers and their traditional core providers will strike a conciliatory tone in 2020 and work together to let the core do what it does best…be boring and reliable…yet develop the ancillary systems and apps that customers demand.

We will continue to see consolidation in this space, not expansion.

CHALLENGE QUESTION

What is your bank's risk appetite for converting to a new core that is unproven and may not succeed in achieving the critical mass of a significant and sustainable user base?

SUMMARY

Avoiding the cacophony of those telling bankers they are dinosaurs who face near-term extinction, smart bankers will succeed in 2020 with the ability to adapt to new technology, scale the enterprise, and sustain their traditional, profitable bank models by adding the right dose of tech and striking the right balance between security and convenience.

Whether they develop or buy the applications customers demand or whether they partner with tech providers who share the same values and approach, traditional yet visionary bankers can and will become the "competitor to be feared."

Here's to 2020, the year that seasoned bankers realize they can do anything a fintech can do…even better.

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.

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