Fall 2022

The Ever-Evolving World of Technology in the Banking Industry

Lindsay Shankle
lindsay.dashae@hotmail.com

The Ever-Evolving World of Technology in the Banking Industry

By
Lindsay Shankle

Project submitted in partial fulfillment of the
requirements for the
Bachelor of Integrated Studies Degree

Murray State University
November 30, 2022

Abstract

In the current day technology is key and crucial to everything we do. Over the years we have incorporated technology into all we have, for the improvement of a product or to make life more convenient. For example, home appliances, vehicles, TV, electricity, computers, phones and even our financials. In order to evolve with the world, we are living in we must adapt to the technology.

Keywords: Innovation of Technology, Customer Service, Security, the future.

Table of Contents

Abstract	i
Introduction	1
Innovation of Technology	3
Loan Applications and Underwriting	3
The Future of ATMs	5
Mobile is Everything	6
Contactless is Coming	7
The Digital Experience	8
Covid-19 Impact on the 9 to 5	10
The Customer Experience	11
Covid-19s Push for the Customers Experience	11
Omnichannel Banking	14
The Baby Boomer Generation	15
Security	17
Security is Paramount	17
Security Tools	18
Types of Fraud	19
Cybersecurity	22
Security Breach Before, During and After	27
Regulations put into place to help Protect the Institution and the Customer	29
Work from Home	30
Millennials	33
The next generation	34
Marketing	35

Embracing Social Media as a form of Marketing 36

Social Media Leadership 39

Cross-Selling 40

Strategy 42

Architecture 44

Conclusion 45

References 49

Introduction

The financial world has evolved rapidly since 1990. An area of particular interest is how it will continue to progress over the next 30 years. In the span of my career of just 8 years in banking I have seen several changes, most of them stemming from the advancements of technology.

Over the past 30 years we have seen both perks and drawbacks of innovative technology. In the banking and finance industries there have been major strides and risks taken by corporations to boost their business past the competition. Some of the innovations include the enhancements of electronic banking, physical and cyber security, core processing systems, new means of marketing, and even the architecture of physical financial institutions. It is recognized that technology is still evolving to this day and will continue to do so for the foreseeable future.

The advancement of technology has given the consumer an easier and real time access to their monies. In today's time we can log in to digital banking and see our account balances and activity in less than 30 seconds. Prior to smart phones and high-speed internet, the consumer would have to wait every 30 days to receive their paper bank statement. Technology has also helped lessen the waste of paper and other resources as many customers have opted for digital or paper-free methods of delivery.

With the development of technology engineers had to learn new techniques to prevent fraudsters from getting consumers' monies, as well as creating core processing systems to house all client sensitive information. This created many new job opportunities for thousands of individuals to manage and develop software and tools to help protect the consumer as well as the institutions. Expansion in one area often has rippling effects for adjacent industries.

In conjunction with security there is also an ongoing down trend of physical money being held in banking locations in result of the new digital contactless world. The need for physical security is still there but it not as demanding as it was in the 1990's. Consumers have less reasons to need to visit a banking center unless the issue that cannot be resolved over the phone or instant messaging. Technological advancements have completely revamped the automated teller machine capabilities, so the days of standing in the teller line with a small paper booklet to withdraw money are long gone. Now with new ITM's (interactive teller machines) all you need is your debit card and PIN number to withdraw cash fast. Major players in the world of finance, PayPal and Square, have released apps like Venmo and CashApp where one will find that paper money is never actually exchanged. Digital transfers pass the same electronic currency back and forth. Marketing has also seen a dramatic and positive change over the past 30 years. Banks used to use radio ads and newspapers to spread the word of their institution and the bill was insanely high. In today's time because of the enhancements of technology institutions have the capably to gain free marketing publicity via social media sites, especially Facebook, and use the advertising budget elsewhere. Even if a banking institute chooses to promote their business through the socials, the cost is minimal compared to the previous amounts spent for air and paper advertising.

One aspect most people would seem to look over is the architecture of banking institutions. In the 1990's banks had larger office buildings and operational centers to hold 300 plus employees (Dixion, 1999). In today's time we can notice there are fewer banking locations and of a smaller size. With the circumstances and repercussions arising from Covid-19 the world realized not everyone needed to be in the office. Many employees began to work from home and

have decided to continue to do so. The innovation of technology is important to understand because it will affect each one of us as consumers as we move forward.

Innovation of Technology

Loan Applications and Underwriting

Bush (1997) predicted technological enhancements would change how loan application would be accessed processed online, potentially hindering community-based institutions that have their foundations built on in-person customer service. At the point in time the article was written loan applications were still processed in person by multiple people, which drove the origination cost of a loan up. Bush (1997) stated the average cost of origination for a loan in the late 90s was $1,600, and the expectation was for this cost to be cut in half in the next five years according to Mr. Steven Williams, the managing director of M ONE Inc. – a consulting firm that specialized in bank management technology planning. The reasoning behind the price reduction was due to the advancements in technology. Williams claimed, “Technology will be used to get the benefit of not re-entering information, of handling bigger workload with the same amount of people” (Bush, 1997, p. 38).

Another noteworthy is how the underwriting process constantly improves. The automated underwriting was a significant development within technology that made the mortgage lending process easier. These applications were entered into the online applications ensuring that all components of loan paperwork were looked at fairly, accurately, and in a timely manner. The government programs that sponsored this technology development platform are called Fannie Mae and Freddie Mac. It was stated that “both government-sponsored enterprises report that more than half the loans they purchase currently come through their automated systems” (Bush,

1997, p. 39). This platform allowed loan applications to be entered and if any information was incorrect or out of date, lenders could update the file and not have to start everything over.

Prior to the creation of these online portals, the loan process was completed manually. Lenders would have to hand write all documents, call to order appraisals, request paper credit reports, all while keeping track of the current stage of the process. With the advanced technology all loan services were tracked and ordered in a timelier manner. Roger Conley, Vice President of technology marketing with Frannie Mae, stated "credit reporting is another area that has benefited from electronic transfer of information, speeding the loan process" (Bush, 1997, p. 40).

It was questioned what the estimated numbers should be for financial institutions to have a website on the internet, and how useful it would be to have the online portals. Warren Myers of Myers Internet Services Inc. supposed, "that around 2,000 financial institutions have websites on the internet, and maybe a couple hundred were community banks" (Bush. 1997, p. 42). Consumers who used the internet would apply to multiple websites, and the company that responded first had a higher chance of getting the business. It was suggested this could hinder some of the smaller community banks that did not have a higher volume of staff in the back office. Myers encouraged the financial institutions to innovate their technology so the whole loan process from application to closing was electronic. At first institutions were skeptical about reaching customers via internet, Myers assured them that "the usage of the internet it much higher than people think" (Bush, 1997, p. 42).

Ashburn, from American Savings Bank suggested "community banks don't see the internet as a viable source of business. But from a credibility standpoint, it's very important" (Bush, 1997, p.44). At this point, community banks were not known for leading the way in technology. They would eventually adapt to new advancements years later, after they saw how

well it played out for larger financial institutions. When smaller community banks did start creating their online applications, Myers noted “the client succeeded in getting seven to eight applications a day within a few months. But the banks legal department raised concerns about disclosure requirements and the institution backed off, giving little information on its website and referring customers to a phone number for more information” (Bush, 1997, p. 44). Even though the smaller institutions saw a rise in applicants they still were cautious, almost like it was too good to be true. However, community banks were seemingly much better off to take advantage of the enhancements because they had a stronger capital base. Overall, the up-and-coming technology of the 1990’s was evolving. It was a first look at how the loan process would be perceived in the future by consumers and the smaller community banks.

In connection to how things were processed in the late 90’s suggested by Dixon (1999). They all talked about a different aspect in banking from electronic banking, security, marketing, architecture and even the banking systems. Thirty-nine people were chosen for the interview in this article. They ranged from the positions of CEO, general managers, Presidents, Chief Operations Officers, banking system creators, and architects.

Chuck White, the CEO of Home Account Network, on the topic of the internet and electronics said “but if banks fail to seize the day they risk losing ground to other financial institutions” (Dixon, 1999, p. 21). To me, that does not seem so farfetched. People always want the next best thing because what they currently have is not good, fast, or new enough. He went on to say that customer would rather deal with real people at their current bank then expanding out to other financial providers for a product. So, if banks did not seize the opportunity, they were in return losing money and customers.

The Future of ATMs

Andrew Harriet, Vice President and Marketing of Sierra Wireless, had the right idea when he spoke about the future of ATMs. He predicted that in 10 to 20 years, wireless data may be considerably faster than most landline-based internet systems. Customers should be able to interact with a real teller from any banking ATM, rather than tracking down a branch for tailored services (Dixon, 1999). With the way our wireless internet service has ramped up the past 20 years, we can literally put an ATM anywhere, compared to then they had to have a landline connection to communicate with the banking system. Not only is the connection better, Harriet called it when he said customers will be able to interact with a real teller. The terminals today have gone from ATM (automated teller machines) to ITM (interactive teller machines); if a client is having issues completing the transaction all they must do is click the help button and the customer will be connected with a bank teller.

Mobile is Everything

In 1965, a man named Gordon Moore made a prediction that computing development would double every 18 months. This today is now known as “Moore’s Law”. Clearly technology has grown exponentially since the year 2000. In just a short amount of time frame we now have high speed internet, we can conduct banking transactions online, and mobile devices have dramatically evolved. With all the changes, bankers must be ready to evolve themselves (Meinert, 2018).

Six key points Meinert made in this article are: mobile is everything, contactless is coming, mobile natives are here, the consumer mentality is always on and instant, banks and fintech firms are collaborators – not competitors and security is paramount.

Breaking down his key points, mobile is everything - Meinert stated that “77% of the United States population owns a smartphone, and many consumers are choosing to conduct ecommerce transactions primarily through their mobile device. Accordingly, the mobile payments experience will continue to play a central role in banks’ overall payment strategies (Meinert, 2018, paras. 4)”. He also noted other sources of payment companies like Apple and Samsung were slow at the beginning, but the use of mobile wallets is still increasing. Meinerts main point is banks need to make sure they do whatever they can to ensure they have a top-of-the-line wallet product so customers will choose them to make their payments.

The mobile natives are here. Meinert makes the remark that in recent years’ millennials are essentially transforming banking, however, even they can still remember the time of dial up internet and landline phones. “The next generation will be different. Members of Generation Z cohort have never known life without technology – they live through their mobile devices, and they’re fast-growing consumer segment. In fact, within the next four years, Gen Z will account for 40 percent of all consumers, and their expectations for fast, seamless and secure banking experiences will be higher than ever” (Meinert,2018, paras. 11).

Contactless is Coming

Little did Meinert know that a year later contactless would be pushed to the front of the line for every technology developer in the country due to Covid-19. “In 2015, the U.S. began the migration from magnetic stripe cards to EMV (enabled chip cards). As a result, more than 2.9 million retail locations today are EMV – enabled, and counterfeit fraud is down 75 percent amount those business and down 50 percent across all merchants” (Meinert, 2018, paras. 6-7). These numbers are a huge success on preventing fraud but the downside of EMV was the amount of time it took to process a transaction. The solution was contactless payments. They created the

chip with a small antenna that can communicate with the processing terminals. Thus, making it faster than having to insert or swipe a debit or credit card. The inclination to use contactless payments is growing quickly everywhere outside of the U.S. Countries such as Australia, the U.K., Brazil and Canada are already running on contactless payments, and the acceptance among consumers is increasing daily (Meinert, 2018). He goes on to discuss how the U.S. is the opposite. The terminals that merchants have can accept contactless transactions, the feature is just disabled. Meinert continues with the increasing demand by consumers to process faster merchants and banks should start putting a plan together to offer contactless. One year after this article was published Covid-19 hit the U.S.; that was the push that the U.S. needed to go contactless.

When the Covid-19 pandemic hit, almost all in person transactions came to a halt to abide by government mandates of no contact. However, it was predicted that when the in person spending recoils financial institutions will want their banks name on the card the customer pulls out of their wallets. Good persuaders to help customers make those decisions are features like perk rewards, cash back and a big one is the tap-to-pay (Gross, 2021). As previously discusses other countries in the world are miles ahead of the United States when it comes to contactless card usage. No with the slow adoption of tap-to-pay there is a wide open opportunity and rewards for community banks. Within the data of tap-to-pay analysis is a profitable trend for unregulated debit card issuers like Visa, which make 40% of non-interest income from debit card interchange transactions. Tap-to-pay debit cards begin to replace cash as the payment technique for smaller transactions (Gross, 2021).

The Digital Experience

The customer mentality is always on and instant. The consumer is always on the bigger and better mindset; this also includes their digital experience. What this means is it is not enough for a financial institution of offer online banking. The financial institution needs to be open to accepting and incorporating new technology. “Payments are at the heart of banks’ digital relationship with their customers, and the more banks can do to make the payments experience fast, easy and enjoyable, the more engaged customers will be” (Meinert, 2018, paras. 13). Research has proven that having more digitally involved customers can affect banks’ bottom line. A Fiserv study showed that having a more digitally engaged consumer generated 16 percent more revenue (Meinert, 2018).

Banks and fintech (finance plus technology) firms are collaborators, not competitors. The relationship between banks and fintech firms was very uneasy at first. Then fintech companies realized the benefits of having financial industries on their side. Banks were known of reaping the rewards of working with smart, knowledge innovators and showcasing exciting new products to their customers. The result of these partnerships is a better customer experience and a greater sense of harmony in the determination to renovate the payments systems (Meinert, 2018). With these two working together, more technology has been created to help make banking easier and comprehensible to the newer generations.

When technology was first invented people are still thinking of how it will evolve next and make predictions. There is the prediction today that physical branch locations will soon be a thing of the past. Rob Morgan (2020) thinks differently. He projected that, why, yes, technology is making it easier for customers to bank on their phones so the physical branch locations will evolve to be more of a service tool then processing transactions. Any transaction from a mobile

app like depositing a check, opening a new account, and even transferring funds can be completed with a phone. Morgan also repeated the suggestion that with Covid-19 customers have become more reliant on being able to bank using their phone with the digital enhancements rather than what the bank offers. But Morgan (2020, paras.4) said despite the enhancements, customers still want someone locally that they can rely on in case of an issue or more in-depth questions. The mention of Apple being the poster child of digitally native companies while they still rely greatly on the physical store fronts for the customer connection.

Morgan also explains how important it is to still have a local person available for customers. “A physical presence in a community gives a brand trust and credibility. It creates a sense of permanence that customers want” (Morgan, 2020, paras. 5). Not only does it create trust and a better relationship, but the customer can also have a better understanding of complex products. In banking there is not a one size fits all. There are some more simple transactional products but not everyone is the same or wants the same thing. Consumers still rely on a face to face interaction for better understanding of what they are signing up for or even for tips on how to use the technology in their hands.

The connections that Morgan is making references instilling trust and credibility, being able to explain complex products, and providing excellent customer service. Banks should learn from these and as time turns, we will slowly see those changes from processing transactions to providing more customer service.

Covid-19 Impact on the 9 to 5

Meinert (2020) published another article discussing how Covid-19 turned everything upside down when it came to the American standard 9-to-5. Some bank employees were able to work from home and the front line however is unable to, and by regulatory requirements banks

must be open or have a source for customers to conduct their business. Guidance was given that banks should look more to local authorities on how they should handle reopening to the public.

The banking industry was serving as a financial first responder, providing a hand when it came to extension agreements on loans for customers who were unable to work, providing small businesses with PPP loans to help pay employees when they were unable to work and helping customer's transition to using technology to continue their financial needs. Most of these tasks would have been nearly impossible if it had not been for the advancements of technology.

Bankers were forced to separate their offices; many began to work from home. In a survey conducted by the ABA (American Bankers Association) in May of 2020, 42 percent of bankers were expected to be back in the office within 30 days, 31 percent said 60 days and 10 percent said they were looking at three months of being able to return (Meinert, 2020).

Prior to Covid-19 most bankers were expected to be in the physical location of the institutions. But due to the government lock downs and social distancing, this forced employees to work from home. Imagine that the pandemic happened in 1995 instead of 2020. This would have been nearly impossible for the banking industry to function due to the lack of technology available at the time. However, because of the advanced technology in today's times we were able to work from home and conduct business as usual, just with a new look. Now that the lock downs have been lifted most of the institution reevaluated having employees in an office setting. Institutions created work from home positions for employees.

The Customer Experience

Covid-19s Push for the Customers Experience

In Colgans (2020) winter addition of the ABA Banking Journal discussed recent events such as Covid-19, have rapidly accelerated the shift of digital banking, and the need for customer

support. Colgan began the article by noting that banks were- and still are- in a rush to find ways to support the constant advancement of not only basic customer needs but also digital needs. “Digital customer problems-solving tools are getting better. Bots are becoming ubiquitous. But even creators of digital customer service solutions say a mix is best” (Colgan, 2020, p. 39). A company called UnBlu, develops hybrid platforms that balance the automation and human advice for financial companies. In the article, Javier Puga, the vice president of marketing for UnBlu explained “having the opportunity to transfer from interacting with a bot to speaking to a human is especially important in the context of complex customer services inquiries that require a level of sensitivity and understanding that chatbots currently lack (Colgan, 2020, p. 39). In the current day many consumers prefer to use the instant message platform rather than call the financial institution. This preference, also a mix of basic and digital needs, explains why platform developers must rush app and web upgrades; until then, financial intuitions must be staffed/equipped with knowledgeable personnel to answer the more detailed questions.

Financial companies and bankers frequently try to find new methods to address the increasing volume of customer questions regarding the enchantments of the digital world. Colgan interviewed multiple bankers to get their input regarding how they handle these situations to provide a positive experience for customers. Scott Miller, Senior Vice President and Marketing Director at Riverview Community Bank, clarified that client services centers must know more than just about the bank products and website. “Besides basic banking, they’ve had to learn, document and describe so many issues” (Colgan, 2020, p. 40). For example, some of those issues include teaching customers to know what type of browser they are using, walking customers through how to enable or disable pop up blockers, what cookies are, and if they are enabled, how to use digital wallet, and how to set up and use PIN, thumbprint, or facial

recognition. Miller stated they have implemented a protocol that everyone who works in the client services center has at one point worked successfully on the front lines at the institution. This helps them understand the products and procedures. “Like in a branch, we utilize our internal gurus, those who understand IRAs or ACH, and others who love setting up digital wallets or helping with Quicken. We do our best to cross-train each other so everyone knows the basics and we know who our go-to resource is as we come upon new challenges” (Colgan, 2020, p. 40).

Miller elaborated further by noting, “the challenge for community banks is having the resources to put all the systems into place. When Google and Amazon are setting the bar for an online experience it can be daunting. How do our community bank clients want to interact with us and manage their finances? Online chat, Zoom/Go to Meeting/ Teams, ITMs, Facebook, Facetime, mobile banking, digital wallets, secured messaging? Or do they want to come see us in a branch? The answer is all of the above” (Colgan, 2020, p. 41). With all these needs, community banks are being forced to upgrade systems to be able to compete with the larger institutions and their customers’ expectations from other experiences and interactions from other comparable systems, outside of the banking world. This can put a strain on their budget.

Community banks feel as if they have been left behind in the past due to the funding and quick advancements of technology. Jelena McWilliams, chairman of the FDIC noted that the challenges community banks are often faced with tight budgets and limited technology expertise. Each bank is different on what they consider due diligence. The cost of technology firms is very expensive and requirements of paperwork and reviews are inconsistent between institution to institution (Colgan, 2020, p. 41). In translation, technology firms are also feeling the strain with

such a rapid growth because no two financial institutions are the same. They must modify their program to fit those institutions policies and procedures.

Overall, this is a good reflection of our current-day struggles with the innovation of technology. Particularly applicable is the unconscious and inherent comparison between our new, improved, digital platform to other frequently visited sites, plus both staff and customer learning curves. In addition to learning the programs, and teaching the programs, staff is still expected to provide customer service, technical support, and banking services. Advancements may have improved some areas, but those advancements have also caused lags in others especially if staff is spending more time helping a customer navigate something digitally. This article highlights the current advancements of technology and how they affect not only the employees but also the consumers.

Omnichannel Banking

Now to stay prosperous banks must adapt to omnichannel banking. Meaning if a consumer can complete a transaction or open an account online in less than five minutes, they should be able to do so in the brick-and-mortar buildings as well. Banks need to adapt to where the consumer and businesses want to bank, unlike the past. Consumers have long looked for convenience and full transparency without having to dig for it.

In the Mantl's 2021 Banking Impact Report, results showed that 92 percent of small business owners thought community banks are just as if not more important to the U.S. banking system as larger banks (Conant & Harley, 2022). Just by offering more state-of-the-art digital products and options. Small businesses are going to be relying on community banks in the upcoming year for products such as invoicing systems, online account opening, and digital

lending. Historically, banks were disinclined when it came to taking on technology and upgrades. They see it more of an expense that may not pay off verses an investment.

In 2021 there was an uptick in banking trends such as cryptocurrency and buy-now-pay-later capability. The institutions who had already been in the digital game were easy to adopt new trends. However, the less tech-savvy banks did not seem to not grasp the concept well. Conant and Harley (2022) suggest,

> More than half of consumers (58 percent) and small business owners (57 percent) will do business with an institution that doesn't offer online account opening, regardless of whether they prefer to open an account online or in-person. Currently, 43 percent of community banks do not offer online account opening for consumers and that figure is even higher for businesses. The message is clear: Online account opening is no longer a nice-to-have feature and the opportunity cost of not modernizing is now a matter of survival. (para. 6)

Without customer's banks would serve no purpose. Consumers want to know they have options available even if they never have intentions on using that specific product. The adoption of new applications and services is broadly used overseas. The banking market is predicted to grow $43.15 billion by 2026 because of the new products (Conant & Harley, 2022). Smaller institutions will need to embrace the new technology to remain competitive. By embracing open banking there will be a significant impact in the U.S. due to the new opportunities that will benefit the consumer and institutions contending with digital innovation.

In 2019, a World Branch Report showed that 51% of consumers had more trust in banks that had branches (Riccio, 2019). The author, Riccio, claimed that trust is going to be critical in the next phase of banking, people will still want the security of knowing there is a real place they

can go to and talk to a real person. Although the branches are there for that level of comforted banks are pushing for customers to take advantage of their digital products. Some banks even did a marketing push and sent customer a $2-$5 check with instructions on how to use mobile deposit in hopes that they will begin to use the product. Kearney Consulting reported that 85% of customers who relied on mobile and online platforms during the Covid-19 pandemic, will continue to do so after (Riccio, 2019, paras. 3).

The Baby Boomer Generation

Holding second place of the nation's largest living generation, baby boomers have a population of 76.4 million (Pulusani, 2022). It is important that this generation not be left behind when it comes to technology. Millennials and Gen Z were raised in the upbringing of the technology we have today, and it comes as second nature. However, millennials only hold 6.4% of the U.S. wealth and baby boomers hold 50% (Pulusani, 2022). Keeping boomers in involved with updated technology and making their customer experience seamless is key.

Making your financial institutions digital platforms and products user friendly and easy is a main concern. Boomers ages range from mid-50's to mid-70's. This means they potentially are managing not only their money, but their parents and children's still. This can be used as momentum to encourage them to use digital platforms. Statistics show that 7 out of 10 boomers use online banking at least once a week, and the use of mobile products is continuing to grow exponentially every year (Pulusani, 2022). This is a prime opportunity for financial institutions to promote products such as online banking, mobile deposit, fund transfers and different payment options to this targeted generation.

Baby boomers are a little more cautious and hesitant when it comes to converting everything to digital. When the 2008 recession hit it impacted their financial positions. This

caused a fear and skepticism in their trust for financial institutions and uncertainties about digital channels and transactions, fraud and security breaches mostly. However, 11 years down the road the Covid-19 pandemic hits. This pushed boomers to adopt newly developed technology to stay on top of their finances. Almost 90% of baby boomers agreed that they will continue to use digital technology to make managing their finances easier even after Covid-19 is over (Pulusani, 2022). With some of the advanced products in today's technology like security alerts this can help to ease the boomers mind, with added customer support from the local branches. Being upfront and transparent with communication about security efforts is a top priority to this generation.

Security

Security is Paramount

On a daily basis personal information is being compromised. Older generations of consumers are more skeptical of using technology because of that reason, a major reason consumers are looking into how their information in being protected. In an ABA (American Bankers Association) poll in 2017 six out of ten American consumers trust banks to safely protect their information rather than alternative payment providers, retailers, or telecom companies. Nonetheless, research also shows that security concerns influence how consumers choose to adopt new financial services technologies. A recent Fiserv study found that 57% of consumers have not used mobile banking, in fear of security concerns (Meinert, 2018). With these key points security and privacy will remain as the core as the innovation of technology continues. Banking regulations are constantly being changed and developed to help protect consumers' privacy.

Hackers are always looking for vulnerabilities in the banking systems. When everything became more digital due to the pandemic, it inspired new fraudulent attacks. Americans have lost over $77 million due to Covid-19- related fraud attacks according to the Federal Trade Commission (Vergara, 2020). In 2020, phishing attacks had increased by more than 667% and account takeover attacks have increased by 72% (Vergara, 2020). Institutions are having to renovate the anti-fraud solutions and strengthen the security of digital networks. Some key suggestions for banks to look at upgrading are e-signatures to securely enable remote transactions, facial recognition for identity verification, preventing account takeover by risk analytics, and strengthening mobile app security.

Consumers do have concerns about the privacy of their information. Westby and Wolf (2019) reported that 7 in 10 consumers said honesty and transparency about how their personal data is used is a part of what they look at when choosing a company to win their confidence. They also reported that 42% of respondents stressed the importance companies with clear communication of their compliance with data regulations, 29% of consumers will avoid institutions who have had a data breach and 63% said they would avoid an institution with a data breach for a period (Westby & Wolf, 2019).

Security Tools

New developments in tools such as e-signatures, facial recognition, risk analytics and app protection have helped enable secure remote transactions and prevent account take overs (Vergara, 2020). E-signatures were a quick and easy product for banks to adopt, as well as faster and convenient. The convince of this product allowed institutions to draw up customer contract request and send them out the same day. Additional options with this product are digital identity

verification. This allowed institutions to offer crucial services like mortgage loans during the Covid-19 pandemic (Vergara, 2020).

Facial recognition is another essential part of identity verification. To exploit consumers, fraudsters have begun application fraud. Application fraud is when an individual applies for a loan with someone else's information posing as them by leveraging personal identifiable information. By banks enabling digital identity verification checks it will help prevent this type of fraud and perceive when hackers are attempting to use imitation identities.

As part of the identity verification enhancement, facial recognition is crucial at being part of the front-line defense. With the use of smart phones consumers have the capability to take a photo of their government issued ID and a photo of themselves to use ID document verification with facial comparison. New biometric comparison technologies with liveness detection verify that the ID is in fact authentic and unaltered, as well as the consumer who is attempting to open the account is indeed who they say they are (Vergara, 2020).

Another key tool being used is risk analytics. Risk analytics is a sophisticated engine that searches for uncharacteristic patterns in consumer purchase indicating new fraud attacks. If financial institutions combine risk analytics alongside their pre-configured rules it can help identify fraud in real time, overall helping the consumer and the financial institution by driving down fraud attacks (Vergara, 2020). A good example of how the risk analytics system operates is a rule or guideline may be in place to increase security if a transaction is over a threshold dollar amount. By complimenting the rule with the learning models that are investigating the device, transaction and data channel it will help identify the irregular pattern. "These models use data points such as the integrity of the device and equally as important, the integrity of the application

– then using the risk score generated to drive a precise level of security for that unique transaction (Vergara, 2020, paras. 10)".

Other combat tools used to help prevent losses on payment cards is the EMV- upgraded chips in debit cards. The enhancement uses a literal chip implanted in the face of your card instead of the mag strip on the back of the card. In a report released in 2019 by Visa merchants who completed the EMV upgrades on their machines saw a card-present payment fraud drop by 76% over a three-year time span (Hoffman, 2020).

Types of Fraud

There are many different types of fraud in today's time with the evolution of technology. One is business email compromise. How this works is an executive or employee of the financial institution will receive an email saying they need to make a significant external transfer. The email verbiage will most likely contain substantial details and swaying language; however, it is actually fraudulent. The message is formed from stolen data and perceived information about a person or their place of employment (Hoffman, 2020).

In an interview about email compromise Brandon Kelly, EVP for fraud prevention at First Bank in Colorado said,

> Account takeovers and business email compromises are also growing in popularity, because scammers have the technological resources and mechanisms nowadays to be convincing in their impersonation of a business or an individual. While there is no limitation of their related exploits, most share a common feature: they are modern day confidence scams. They target users to gather personal information and can leverage real-time payment networks to move money quickly. Business email compromise also

> succeeds from misplaced trust, in this case on a channel that was designed for convenience rather than security. (as cited in Hoffman, 2020, paras, 4)

Even more reason why financial intuitions should make the investment on their digital platforms to help protect customer's information and the banks reputation on security.

Paul Wilson, the director of anti-fraud products for AppGate, recommended the best way to battle this growing fraud type is to confirm with the requestor via phone call or in person, due to the fraud preventative tools not always catching the spoofing (Hoffman, 2020).

E-commerce/card-not-present is another rapidly growing fraud due to the growing amount of online shopping. With the EMV chip enhancement it is making it a little harder for physical POS (point of sale) fraud more difficult. Scammers are having to resort to online transactions of card not present, meaning you can type the card information in (Hoffman, 2020). Over time the liability for fraudulent transactions have transitioned from bank card issuers to the merchants. Merchants have become aware over the time frame to be more alert for scams. The number of chargebacks and disputes are not only inconveniencing the merchant but the customers as well. Cyber criminals have also learned how to steal information retrieved from online merchants and sell it on the dark web (Hoffman, 2020). According to a report by Javelin Strategy & Research card-not-present fraud is now 81% more likely that point-of-sale fraud (Hoffman, 2020). How funds were being spent during the Covid-19 pandemic were a significant shift then how they were spent prior. Everything was processed as card no present for the contactless requirements.

Authorized push payment fraud or APP fraud happens when a consumer or business is persuaded or coerced into authorizing a regular or on-going payment to a fraudulent recipient. With the increase of real-time payments, this has made APP fraud more appealing to criminals.

In the U.K. where real-time payments have been established longer, APP fraud jumped 44% in 2018. In January of 2019 the U.K. Financial Conduct Authority executed a rule permitting victims of APP fraud to complain to the receiving payment service provider, the fraud still grew. Over $207 million was stolen from victims who were coerced into authorizing a payment then ended up being an AAP fraud schemes in the first half of 2019. That is up by 40% from the first half of 2018 (Hoffman, 2020).

Synthetic ID account creation is when fraudsters will create a realistic fraudulent account or identity with a combination of legit and falsified information. “According to a study from Lexis Nexis Risk Solutions, 86% of fraud losses experienced by mid-to-large online retailers involved the use of a synthetic ID accounts (Hoffman, 2020, paras, 15)”. Financial institutions are focusing on initial account opening underwriting processes to help prevent false accounts from being opened. Social media also provides data for fraudsters to exploit. Banks and their third-party suppliers need to continuously work through debit card purchases and modify the fraud detection engines, stated Paul Tomasofsky, a partner with McGovern Smith Advisers (Hoffman, 2020).

SMS spoofing is when a cyber-criminal impersonates a trusted third party by sending the victim a message that appears to be from their bank or merchant to follow the payment instructions. This technique of fraud is also growing with the rate of online shopping. Customers rely on messaging to make and confirm the payments (Hoffman, 2020).

Cybersecurity

Financial institutions are a huge cyber-target due to the sensitive information they possess. The traditional cyber security defense focused on perimeter defense, protecting on-premises systems, and compliance requirements. Defense software is constantly having to

develop against cyber threats to protect the sensitive information. Now banks are migrating to using the cloud to transport and store data. The benefit is it is much easier to access and cheaper to store, although the more data the more problems can arise. The amount of data being generated is causing a strain on the cybersecurity teams. There is the same amount of information, but it needs to be monitored much closer and more frequently (Daniels, 2021).

Research completed by Markets Insider shows that financial firms face as many as 300 times more cyber-attacks than business in other divisions (Daniels, 2021). This information is completely understandable due to customers using digital channels to complete their banking needs as well as the financial institutions switching their processes to the cloud. In May of 2021 Wall Street's six largest banks CEOs appeared before Congress to discuss the position of the nation's financial system. They named cybersecurity threats as the greatest current risk factor (Daniels, 2021). Once more due to Covid-19 and the rush for financial institutions to update and upgrade technology so employees could work remotely, it left a gaping hole for cybersecurity protection. Prior to Covid-10 financial institutions focused on the traditional cybersecurity needs such as perimeter defense, protecting on-premises systems, and compliance requirements. However, that is no longer enough in the new digital age to protect against cyber-attacks. This new transition requires robust people, procedures, and technology.

Business even outside of the financial realm have adopted the use of the cloud and digital workforce. The relocation of data and processes to the cloud is improving the customer experience, improving in-office efficiencies, and encouraging competitive advantages. As they say with great power, comes great responsibility. Cybersecurity is no exception. The amount of information that is being produced in the financial world is putting stress on cybersecurity teams because of the constant reviewing needing to be completed for routine cleanliness checks and

susceptibility scans (Daniels, 2021). Further Daniels (2021) found that large banks spend around $600 million each year on cybersecurity programs, and they have more than 3,000 employees working to advance the strength of their cybersecurity. Moving infrastructure and services to the cloud was inevitable. The operational and cost-saving benefits of the cloud have seduced many organizations to migrate their data. Still, the rapid spike in adoption due to the impact of a global pandemic was not part of the budget or plans (Daniels, 2021).

Recommended best practices for banks to advance their security are developing a cloud-specific security strategy, test it and then test it again, control artificial intelligence and take a rounded approach. It is unwise to use the same security tactic for the on-premises system as the cloud environment. Banks need to establish a solid policy around what sound cybersecurity should be for the cloud, weather it is a private cloud or public cloud they have opted to use. It is best practice to establish this policy before the company migrates their systems.

When it comes to testing the product, it is better to find the flaws and holes before you go live with you customers. It is also best practice to have a fresh set of eyes test out your product in case there is a defect that was looked over. When it comes to protecting your customer against fraud or a threat of cybersecurity issues it is not a one and done activity. Just as technology innovates, so do the threats and the susceptibility. It is best to continuously have soundness checks completed by staff or by a third-party vendor that is experienced in this field. Artificial intelligence has grown profusely over the years. It is helpful at detecting and analyzing insights from large volumes of data.

However, it does not replace the intellectual thinking of the human role for cybersecurity. Most of the time these ideas of an easy fix are over sold to companies, and it ends up being a

failure. Human intellectuality is irreplaceable in the cyber world. With skills to analyze and put themselves in the shoes of the hacker to predict what their move will be.

With the Covid-19 pandemic many employees were set up and forced to work from home (Hoffman, 2020). That was a transition most institutions were not prepared for. This change affected how the daily operations were handled, as well as the security across the board. There was a sudden need for laptops and mobile devices that employees used for work off premises. The financial world has been forced to push the fast forward button to be able to continue conducting business. This includes high up executives all the way to back-room staff. In "normal" times companies only had to worry about securing the company systems, now they must worry about the computers and devices on unsecured internet networks. This posed a different threat that had to be solved very quickly to follow the governments mandates.

At Javelin Strategy and Research in 2020 Mathieu Auger-Perreault, the director of fraud and security stated that there was" (Hoffman, 2020, paras. 1). The door for vulnerability has been swung wide opened. To help prep staff who were sent to work from home Jeremy Baumruk, the director of professional services at Xamin helped his financial institution clients aggressively educate their employees on password education, patching and good cyber hygiene (Hoffman,2020).

The Covid-19 pandemic reveled on how small of an operation with cybersecurity can transform into a key factor. David Kelly, with FirstBank in Colorado advises on important points to look at when you use a third-party vendor. One being you must understand what the third parties' responsibilities are, how they are interconnected and how they are going to develop over time. Research their incident response, their cybersecurity and how well are going to respond. Kelly went on with 'if they don't have the right capabilities, such as if their services go offline,

that could impact you drastically or potentially compromise you on some levels (Knudson, 2022, paras 14).” What this entails for the financial institutions risk and IT department is not only reviewing the vendors but their institutions risk profiles often and comprehending how changes will influence their company.

The risk of ransomware puts a piercing fear in financial institutions, that is why it is important to use a robust vendor with strong product resilience. Ransomware can infect the third-party vendor and perceive the financial institutions data. The risk is now not only with the financial institutions network but the third-party vendor as well. With the huge acceptance of digital adoption over the past two years third party vendors are significant more now than before to banking operations.

In preparation for a security breach the role of a compliance department is to have a plan in place prior to a security breach to help serve as a resource in helping management execute the institutions incident response plan (Westby & Wolf, 2019). This established plan will help guide the employees to identify likely customer information that has been breached as well as harm to the customer and institution. It is best practice for the compliance department to review and reiterate the plan, lay out expectations and have resources on a regular basis.

When the word “security breach” comes up, it is often accompanying with a cybersecurity risk. A security breach causes harm to a financial institution. Depending on the magnitude and involvedness of the financial institution the chief information security officer, an information security department or a committee may be in control of the data that contains the personal identifiable information. Although one of these officers or departments have the principal responsibility for the customer’s information data not all security breaches will be

handled by that sector. An example was given for further clarification. Westby and Wolf (2019) suggest,

> Should a systems vendor error expose the names and addresses of the bank's significant customers to the vendor's other customers, the breach may fall under your incident response plan. It should still be reported and evaluated by the appropriate areas of the institution, but information security may not be taking a lead role in that incident response. An institution's incident response plan should include sufficient representation from across the bank to allow for appropriate breach assessment and response. (paras 6)

Compliance contributes to the role of protecting the financial institution by helping minimize the risk. The department is frequently accustomed with the interrelation between reputation risk, operational risk and compliance risk by being in the role of the day-to-day risk for the institution. With a proper plan in place the compliance team can be the strategic partner to the information security, marketing and the others who are involved with the incident response team to act fast and in a timely manner (Westby & Wolf, 2019).

Security Breach Before, During and After

Prior to a security breach financial institutions must have an action plan in place. With the experience of working on regulatory compliance change management and compliance issue resolutions, a compliance department is a valuable resource to have. In the event of a security incident compliance can help by identifying internal participants and lead cross-collaboration. The knowledge they have with addressing diverse sources of control failures across the bank that are contributing to a financial institutions issue is extensive. For example, automated systems versus manual processes, internal versus external failures and employee knowledge versus customer confusion (Westby & Wolf, 2019).

If a security breach were to happen some of the situations to address are assess the nature of the security incident, consult outside legal to prepare the litigation risk, seek advice from external consultants with expertise in the type of breach and be sure to notify regulators. Many cyber risk insurance policies include right to use to a legal cyber incident coach to help guide a response and provide legal coverage. The response team will also need to ensure that there are detailed records of the institutions plan of action and evidence of system settings, detection logs and event logs are retained. It is also suggested that communication also be tracked between the senior management and board of directors. An evaluation of the potential impact on the institution and customer needs to be completed, as well as the risk of identity theft. A clear line of communication to the public, customers and staff needs to be established (Westby & Wolf, 2019).

Post-breach, compliance can help management understand the value in risk evaluation and identification of controls improvement. Banking institutions understand that just like technology, breaches are also always evolving, and no financial institution is resistant against them. After the fact, management may want to spend adequate time reviewing how their financial institutions response team handed the breach. Management will also have real experience from which to call back on when it is time to re-evaluate the procedure. Compliance can also be proactive and encourage the change for financial institutions who are more reluctant with modifications. They can also work alongside the department who was affected as well as any vendors. Smaller incidents may encourage informal conversations or may be brought up at the next risk assessment discussion. Depending on the size of the incident and severity, it may be essential to obtain counsel to ensure the intuitions own interest are protected.

When the institutions risk assessment happens, they will evaluate any incidents that posed risk to the institution. This includes both the reasonable impact and the probability of the institution suffering the impact. In the discussion compliance should ask: Did the policies and procedures effectively guide the institution in addressing the situation timely? Did the institution follow the protocol that is in place? In more detail was the breach reported to the right channels? Was management notified timely? Was the institutions' reaction receptive to the risk that emerged? Was the institutions incident response team in place to evaluate the situation? Did other controls function as was expected? Were the affected vendors responsive and accountable? After a thorough review and appropriate changes, if any, the financial institution should adapt and prepare of future attacks (Westby & Wolf, 2019).

Regulations put into place to help protect the Institution and the Customer

Under the Gramm-Leach-Bailey Act, the Right to Financial Privacy Act and the Fair Credit Reporting Act financial institutions are required to protect all non-personal information in connection to any current or former customer. However, Gramm-Leach-Bailey Act does not preempt state law if the law is consistent with the Gramm-Leach-Baily Act and if that statute give customers more privacy protection (Westby & Wolf, 2019). Financial institutions must have a clear understanding of what is expected of them and requirements for consumer's privacy. In today's time financial intuitions and businesses in other sectors contain more personal information than ever before. It is predicted that the amount of data will likely increase as will analysis methods to use the data with technology still being developed. Although some of the data can offer protection there is still a risk. Criminals and fraudsters are constantly seeking ways to abuse systems weaknesses to misuse the information they possess (Westby &Wolf, 2019).

For the foreseeable future institutions should prepare for additional examinations on consumer protection, the effectiveness of their compliance department and tighten up on fundamentals surrounding Anti-Money Laundering Act of 2020 that will be enforced for 2022 (Knudson, 2022). Ryan Rasske the American Bankers Association Senior Vice President and risk expert advises that compliance officers enhance their existing partnerships and deploy automated systems that can help the business manage its compliance programs. It is also hard to find competent compliance professionals in today's time, especially if the institution is adding technology, the cost will only increase (Knudson, 2022, paras. 15).

Another push for the upcoming year is how banks handle fair lending regulations on the racial inequity and differential treatment on transactions they consider fraudulent. With the Covid-19 pandemic there was an increase of cybersecurity fraud and fraudulent debit card transactions. The question is the financial institution putting holds on accounts because they consider it to be fraudulent activity and is it being completed in a way that's disproportionately impacting only certain people. Regulators encourage the financial institutions to look at their deaccessioning factors through a risk management point of view (Knudson, 2022).

With the upsurge of technology, the past two years increased the risk of ransomware and similar threat vectors which in return added additional regulatory requirements. Such as, a possible reporting requirement and potential fines for the lack of certain reporting and even 24-hour reporting for suspected ransomware attacks. Benda Mulvey, a managing director at Promontory Financial Group's compliance practice said there is legislation talk that will to his knowledge not specifically target the financial institution. However, it can potentially hinder the relationship between the financial institution and third party vendors. Simply due to the fact of

straightening out where the line falls between on who's reporting responsibility it is, the financial institution or the providers (Knudson, 2020, paras. 13).

Work from Home

With the push from Covid-19 financial institutions were involuntary forced to allow employees to work from home, prior to Covid-19 this was rare. For example, the 230-million-dollar asset State Bank Group headquarter in Wonder Lake Illinois has 75 employees and only on occasion do any employees work from home. During March of 2020 the Chief Executive Officer, Michelle Toll said that 70% of the staff was transition to a work from home position to continue business and follow government mandates. They had to work quickly to adapt fast because prior to Covid-19 around only 40% of employees had access to be able to work remotely (Hoffman, 2020). What helped State Bank Group out was five years earlier in their pandemic and business continuity plans they developed a specific plan to begin using a virtual server and desktop environment. This allowed them to be able to release the employee's devices much more rapidly and securely than other institutions.

Although working from home away from co-workers in the begging of 2019 was necessary, in current day of 2022 it seems to be the new normal 9 to 5. Financial institutions have started to plan on how to best implement a work from home position to recruit and retain talented employees. Stephanie Bowers, the chief legal officer and regulatory counsel at USAA said the first rule of thumb is to maintain an open line of communication (Hintze, 2022, paras. 6).

When everything was switched to the work-from-home positions along with the technology push there was also a need to create guidelines for what is expected of employees. At first there was childcare issues, parents having to complete their work while also watching their children and let us not forget the boundless Zoom meetings. Bowers added "an open-door policy

is paramount, even if that door is virtual. To understand employees' and peers' concerns about balancing home and work as well as their work responsibilities (Hintze, 2022, paras. 6)." Bowers even came up with the idea of "virtual hallways", this included a extra 5 or 10 minutes before or after the meeting giving the staff time to refill their coffee or chat with a co-worker similar to the in-person meetings.

The issue we are working with now is that older employees may enjoy this inneraction because they are more established in the company. Newer employees might prefer the hybrid model where they have at least one in-person interaction a week. Robert Iommazzo, the managing partner and co-founder of financial services focused SEBA Executive Search stated that younger recruits may be more attracted to organization who provide more of a social life as well as mentoring and networking to help advance their career (Hintze, 2022, paras. 10).

Other concerns faced with the hybrid work from home position includes employees feeling isolated and being able to maintain relationships between the companies' lines of businesses. Bowers plan of action to fix some of the issues is to meet on a regular basis with her department and peers, such as internal audit to discuss industry trends and internal issues they are facing (Hintze, 2022).

Dameshia Mosley, a deputy director of compliance said they are forming their hybrid work-from-home position around a serious understanding of expectations from the employee and employer as well as what motivates them. It is important to understand what is working well and share the information with the department heads to assist minimize any informational gaps and ensure a smooth transition (Hintze, 2022, paras. 15). Mosley has a laid-out beta plan to go over what works well and what does not over the next 6 months. Involving the Human Resources department immediately is highly important, to ensure the hybrid work-from-home plan does not

violate and current policies. Human Resources can also assist with creating the parameters for issues such as hourly employees and that they are not working excessive hours. Another cause of concern is employees with in-person issues are doubtful to improve when working remotely. Additional criteria to consider as a requirement for the job would be does the employee have adequate technology to make this position work. Other perks to consider offering are educational benefits, reimbursements to sign up for online fitness application or gym memberships, allowances for mental-health support services and even making healthy food choices (Hintze, 2022, paras. 21).

Bowers made a final comment "I don't see us ever as a nation going back to a one size fits all approach, in banking or in business. The more flexible and empathetic we can be as colleagues to each other, the more I think we can fulfill the mission of the organization and also meet the needs of the various stakeholders (Hintze, 2022, paras 26)." The pandemic seems to have made the hybrid work-from-home position a more favorable model moving forward.

Millennials

In a survey of private banking clients that are millennials (born between 1981 and 1996), 46% said they are unhappy with their current wealth management benefactor (Chung et al., 2022). Their disappointment to blame on the unfathomable fees, unattractive products they are offered, unappealing investment recommendations, difficult digital process and the lack of customer service.

By 2029 millennials will outnumber all other age groups in the workforce. These tech savvy natives stand to inherit more than $22 trillion by 2042 according to Cerulli Associates (Chung et al., 2022). Until financial institutions decided to tighten up their game and provide the right products and services that are worth what they are asking, they will lose a good chunk of

their customers in the years ahead. By using a tiered service level joined with transparent pricing and excellent customer service with a good experience private bankers will thrive.

According to a survey 80% of millennial private banking clients said that they are currently or considering on using fintech services to help them manage some of their money. Millennials plan on apportioning more than half of their investments with fintech wealth managers (Chung et al., 2022).

Millennials are looking at quality service and product for an acceptable price. It may seem they like to price shop; however, they just want to find the best quality that is not over or under priced. Another survey revealed that the quality of product and services consistently ranked the highest of importance above the suitability or brand. Millennials also ranked price at the lowest, because when they feel the quality is right, they will pay for it (Chung et al., 2022).

Along with quality service, millennials are looking for a personalized banking experience with someone they can relate to and trust. They not only want their banker to be knowledgeable with experience, but they want them to match their interest and personality. This has challenged private banking institutions to produce ways to connect and match private bankers with their clients. For example, some institutions have created a matching tool for their clients. Rather than walking into a bank and being blindly paired with a banker, this tool gives more control to the clients. The client has the ability to swipe through banker profiles until they find one they believe will be a good match for them. This allows the customer to feel more connected and willing to share more with the banker of their choice (Chung et al., 2022).

The next Generation

Generation Z is commonly known as the younger generation. However, the eldest of Generation Z are entering the workforce and their buying power is growing. Generation Z is also

the first generation to be 100% digitally instinctive. With this in hand companies not only financial are changing how they encounter as well as operate. According to a recent study, generation Z and millennials are less likely than baby boomers to completely trust their banks and that trust and security were leading influences in choosing their bank (Whitcomb, 2022).

Generation Z thinks about their finances differently than baby boomers. They take a more digital approach. By financial institutions embracing modern digital resolutions that are more protected, dependable and seamless as well as meeting the customer's needs, they develop a stronger trust with the customer (Whitcomb, 2022).

Most adults say they were satisfied with the financial institution. But in a 2022 report by Morning Consult survey research conducted in 2021showed that some customers believe they are not getting enough financial support from their institution (Whitcomb, 2022). When the Covid-19 pandemic hit there was a cumulative gap in financial literacy and financial well-being. In a survey conducted by the Federal Reserve showed that one-fourth of adults were worse off monetarily than 12 months prior, and this is the highest since they began collecting the information in 2014 (Whitcomb, 2022).

In the past financial institutions would encourage financial literacy. They would give customers tools of guidebooks and teach classes to help them improve their financial well-being. Generation Z and millennials have shown an interest in financial institutions providing automated financial guidance or even virtual assistants to help them understand and manage their finances (Whitcomb, 2022).

Marketing

In an American Bankers Association survey of bank marketing leaders revealed that there is going to be an organizational shift within financial institutions marketing departments. In order

to increase revenue banks will increase and broaden its marketing emphasis on technology driven campaigns. The role the marketing department will have is to accommodate this focus and increase engagement (Gibson, 2022).

Wendy Kagan, Executive Vice President, and chief engagement officer at Bank Newport bring up that her bank has seen a significant shift in brand building over the years. Recently they have invested in technology call CRM (customer relationship manager). This technology will allow the automation of cross-sell campaigns based on personalized product modelling (Gibson, 2022). This can help increase the customer's experience. Approximately 65% of banks have devoted in a customer experience role in their marketing department, while 55% say that marketing is for data and marketing technology management (Gibson, 2022).

In the same American Bankers Association survey, it was collected that 70% of financial institutions said they use outside resources to help them navigate the new data and technology developments, as well as 72% of marketing activities (Gibson, 2022). Activities like digital and social media advertising, public relations, and content marketing. Financial institutions are also investing in SaaS (software-as-a-service) providers to help fast-track the marketing and sales process (Gibson, 2022). John Barron, chief strategy and growth officer of South Shore Bank stated "the days of large scale on-premises installations are likely numbered (Gibson, 2022, paras. 14)". Financial institutions are incessantly trying to increase growth through digitally focused curriculums by using programs like SaaS (software-as-a-service) as a marketing computerization center (Gibson, 2022). Marketing leaders who were interviewed for these surveys agree that marketing is playing a bigger role in helping the financial institutions reach revenue growth goals. To complete those said goals financial institutions are going to have to invest in analytics, technology and digital marketing techniques (Gibson, 2022).

Embracing Social Media as a Form of Marketing

On the marketing standpoint Paul Fiore the founder of Digital Insight, prediction of the future is chillingly accurate. He said “already entering the marketplace are online software engines that can implement one-to-one marketing strategies based on individual customer preferences, transaction histories and permission profiles” (Dixon, 1999, pg. 27). Today we can google how or where to find something and the next thing we know we see an ad for that on Facebook. Paul went on to discuss how banks and financial services can play into this software to help with product sales. They can learn what as cited most asked for product is and evolve their institution into offering that said product.

In the present day, companies are trying to cut back on advertising budgets. However, an American on average streams around 8 hours of content per day. With this being stated, what is the appropriate means for advertising? Oxford (2020) implied that print is not the answer, on the occasions you might read the paper you will notice how thinner and thinner it becomes. Social media is a better option, except statistics show that social media is not viewed on computers it is mainly view on mobile devices. So, when creating the platform, they recommended you create the layout to be viewed accordingly. TV is still an obvious option with advertising, the struggle is to choose between cable, streaming, or broadcasting. The decision maker is what audience are you trying to reach? The answer will help determine the cost and the best platform. In the early 2000’s their options of advertising were very different. Most of the options were in print. With the technology developments over the past 20 years, we have been given new outlets to reach different audiences.

It has never occurred to me that this part of technology could have such an influence. Wilber (2020) delivered statistics about the effectiveness of social media can play a role in the

company, “In one survey, 78 percent of U.S. readers of financial publications said they felt it was important for CEOs to communicate about their company using social media” (Wilber, 2020, paras. 1). The takeaway was not that they had to lead the way and make the actual post, but to set the standard and show their involvement. Employees look at the CEO as a role model and if they are not participating why should the employee. Wilber laid out three ways CEOs can help lead their teams, by embracing innovation, leading by doing and support all social initiatives. All banks have different departments of employees who specialize in an area, for example marketing and retail development (Wilber, 2020). These two markets work together to innovate new technology to better serve the customer. Social media posts by the marketing team roll out these newly adapted products or advancements, then the CEO can include a statement to show their support on the work and product. The CEO can lead by sharing the brand’s content to build a stronger relationship with the consumer. This will set forth an example for the team to do the same. By supporting social media banks can use it as a form of communication to consumers. They often use the platforms for communication, scam alerts, marketing, and sales.

Financial institutions are having to prepare to adapt their strategies to be effective on social media. In a report release by the American Bankers Association, 40% of respondents said they have applied a plan for how frequently they post on social media and only 19% said they have a clear goal for their social media efforts (Ren, 2019, paras. 1). To stay relevant viewers are not looking for visual and informative content, instead the unique and unusual post are more likely to be remembered.

To boost social engagement People Bank located in Washington posted on their Instagram page for the community to participate in a three-week scavenger hunt of 250 piggy banks hidden in their service area. To spur the engagement from the community, People Bank

would post clues on the Instagram page and offer incentives like sunglasses and an entry into a prize drawing for piggy banks found. The result of this social media push encouraged viewers to visit the community parks, increased the interaction on the banks website and even the physical location. By financial institutions using social media for your not so average ads and posting about involvement in the communities, contest, congratulatory events and awards for locals and promotions of banks sponsored event they are reaping the benefit of free advertisement and gaining potential clients (Ren, 2019).

Natalie Bartholomew the Vice President and Chief administrative office of Grand Savings Bank said that “sharing photos of employees is an effective way to attract like and generate conversations on social media” (Ren, 2019, paras. 9). Bartholomew was able to considerably increase the total number of Facebook followers in two years by repositioning the strategy and removing any type of content that had zero engagement. She stated they find this information by looking at analytics on social media post performance. With everything good of cores there is a bad, opening the door on social media will unavoidably cause some customer frustration to surface. The financial institution should have a proper plan into place and be able to respond. Bartholomew advised that a situation can often be defused just by going on social media and acknowledging the negative comment (Ren, 2019). Financial institutions have also received positive feedback having employees promote content on their personal platforms. It helps the viewers see a more holistic view of the company and approachable feel of the bank.

Social Media Leadership

In a survey of U.S. readers of financial publications 78% said they felt it was important for the CEOs to communicate about their company using a social media plat form (Wilber, 2020). However, this does not mean that the CEO needs to direct the social media page on a

daily basis or create every post. What the survey collected was that the CEO can lead by example and set the precedence for a more social media presence for their institution. In the same survey it was also noted that one in four CEOs have an active social media account (Wilber, 2020).

The average age of a financial services CEO is 60 years old (Wilber, 2020). This could be one of the main reasons we do not see as much of a presence on social media. The younger and more tech-savvy generation, mobile technology and social media is second nature. Another enormous reason could be because of the FINRA (Financial Industry Regulatory Authority) regulations for electronic communication. Intuitions can face fines for compliance violations. One of the largest fines to date was a total of $2 million dollars for a compliance violation (Wilber, 2020). Though with the proper training and best practice policy it is easy to overcome these apprehensions. The enormous value that a social media platform can boost your brand is well worth the effort and sweat.

A consumer survey on digital banking discovered that 15% of customers are now "mobile dominant" and mainly use their smart phones for banking. They also expect to be able to contact their banks directly through mobile as well via instant messaging through the app or social platforms (Wilber, 2020). Just like technology evolving over the years so are the customers. The leaders who recognize this and adapt to change for their institution prove to their customers they are open to acclimatizing how they do business.

The leading by example method is a strong selling point. This can be done by having the bank employees share branded content on social platforms to help build a relationship with customers. Although getting employees to participate can sometimes be the problematic part. If the CEO sets the tone and remains active however, this could boost the involvement.

Full support is another high note. The CEO cannot half commit to having their institution have a social media presence. Social platforms can be used for things like customer communication to inform them of location closing and reminders for holidays. Of course, there is always marketing and sale and even risk management. Having a clear understanding of the effectiveness social media can have on your institutions marketing employees jobs an invest in those tools and resources that they need to be able to do those jobs efficaciously.

Cross-selling

There is often a missed opportunity when it comes to social media. One of those being able to cross-sell. In a survey of around 300 financial institutions found that 64% of the respondents are not using data to cross-sell to their existing customers (Wilber, 2022). The capability to collect and act on current customer's data to cross-sell can create revenue for banks. On average a borrower will obtain at least 11 mortgages in their lifetime and lenders retain fewer than 20% of their past customers (Wilber, 2022). This is a targeted opportunity for mortgage lenders and financial institutions to build that relationship by cross selling. Persuade that customer when they close their loan, they should also open a checking and a savings account. Financial institutions are missing out because they have their hands into many areas.

Understanding the financial institutions audience and what is important to them is a key factor. Financial institutions can track things like comments, likes, shares and click-through that possess valuable perception. The information can tell you about what content is connecting with your existing customers and where there is potential cross-selling. The main thing to remember is cross-selling to a current customer is 60% to 70% while cross-selling to a new potential customer is only 5% to 20%.

Another strategic tool to use is being able to communicate with a targeted group of customers. By collecting certain data and composing a targeted list within the customers the financial institution will be able to cross-sell certain products. When targeting a paid ad, you need to ensure it is at the right time and send the right message. For example, pushing ads targeting first time home buyers. Then once they close on their loan a year later, they may see an ad for a home equity line of credit for home renovations (Wilber, 2022).

Keeping the content relevant will keep your viewer engaged. The data you can collect will also tell you which customers have not been as active (Wilber, 2022). By using paid social ads that send a reminder to your customers why they chose your financial institution in the first place. This also gives the ability to showcase new product you have to offer. Re-engagement pushes should have a dead-end, they should lead your customer to continue further. For example, a post about home buying tips will attract customers who are looking into buying a home. If there is a link to a landing page of a first-time homebuyer's guidebook, with the option for the customer to put in their information to be contacted by a lender. This can prompt staff to make a follow up phone call and potentially gain business.

A recent research study showed that 27% of Baby Boomer who are pre-retirees intend on working part time during their retirement with zero plan to stop working all together. This will encourage them to stay intellectually engaged and preserve additional income (Pulusani, 2022). The marketing point of this statistic can be used as a tool. The extra disposable income can encourage this generation to purchase new vehicles, home renovations or even take vacations. This is an opportunity of financial institution to market these products towards not only the workforce generation but the boomers as well.

Strategy

As research has shown social media can be a resourceful tool used to enhance marketing and business objectives. It can help build new relationships and better the current. Six recommended strategies to help increase engagement on social post are to make sure you are picking the right networks, engage your employees, encourage your customers and community members, run social campaigns, be relevant and helpful and paid media (Farley, 2015).

Picking the right network is crucial. Not every financial institution needs a presence on all social platforms. The first step it to identify who the targeted audience is and develop your stance on those platforms. Then deciding the type of content, you want to post. This can range from text content like articles and share similar post to visual content like photos and videos.

Engaging your employees is no easy task. The proper internal cooperation is needed to be effective on the social platforms. When you launch or decided to expand your companies social network you should encourage your employees to be excited about it. Communication with internal staff prior to launch is best practice. The average employee can likely reach 10 time the amount of people that the financial institution can just by sharing the information on their own pages (Farley, 2015).

Encouraging your customers and members of your community to be active on social platforms can encourage them and most likely become your biggest supporter. Let them know your platforms and invite them to join or follow. When you send out email pushes include links to the social platforms and your web pages (Farley, 2015).

Social campaigns are an easy way to attract a social following by including incentives to connect with your bank on social platforms. Ideas such as a form of a contest, giveaway or even a sweepstakes. However, it is important that you stay in compliance and choose an incentive that

is in your banks policy. Also, if your choice of campaign impacts the community in a positive way or benefits an organization there is a stronger case of building a stronger following (Farley, 2015).

Being relevant as well as helpful with your post helps get your audience engaged. If the content fits them and their needs, there is a higher possibility they will participate. There is an opportunity that is created when your content or post receives a like, share or comment. It becomes visible to others who may not have originally seen your post.

Ideally creating your own organic post is more profitable. Although if it is not gaining the traction your company is looking for there is always paid media. Most social platforms offer the capability to run ads to a distinct targeted audience. Paid advertising along with other marketing campaigns will help increase your customer's interactions.

Architecture

Architecture is one thing people often look over when it comes to financial institutions. It was probably assumed the buildings were the same as they have always been, just minus the technology. Jim Givan, the President and CEO of Design Build Concepts advised in 1999 that twenty-five years later customer would perform their banking needs on a PC and the teller line may as well be extinct (Dixon, 1999). If you notice in financial institutions today newly built banks tend to have less of a teller line and more of a one stop spot for all of your transactions. Tellers are considered customer service representatives, who can answer all of your questions. The lobby sizes are much smaller than older banks due to the reconfiguration of adding office spaces (Dixon, 1999). Jim also mentioned that there will still be a need for the drive-up service windows.

Conclusion

The enhancements that have been developed in the past 30 years have helped reshape the way our financial system functions. The enhancements of electronic banking, physical and cyber security, core processing systems, new means of marketing, and even the architecture of physical financial institutions have proven to benefit both the financial institution but most importantly the customer. Newer laws and regulations have been developed to coincide with the developments.

At the institution where I work prior to Covid-19 we went through what we called "innovation". We made a huge move switching our core system and upgrading our technology for the very reason to stay competitive and offer the best products. Our new debit cards have Apple and Samsung wallet capability as well as the tap and go feature. Along with those upgrades we also gained our own P2P (person to person) transfer capabilities, it functions very similar to PayPal and Venmo. It was a choice we had to make in order to stay in the new technology world.

With all of the enhancements of technology there were and will be in the future growing pains, but once past those the financial institution and customer will have an overall better banking experience. With the benefits of upgraded technology, we are able to provide faster service at our teller windows and drive through as well as our customer service desk. Prior to our upgraded system on average, it would take around 20 to 30 minutes to open a new account. Now it takes 5 to 10 minutes' tops to open the account, set up your online profile and walk out with your debit card. The new and improved technology is easier to operate and understand.

Covid-19 concerned me and staff greatly in 2020. Overall, this was harder on most consumers because it forced them to go digital. This meant more online account opening verses

in person account opening. The lobby wasn't accessible to the public forcing customers to call in with more questions and concerns. Normally we would set the customer up in person with a new account, a debit card, online banking, direct deposit forms or anything else they needed. Now this was done limitlessly due to the pandemic. Our goal as a bank is to maintain top notch customer service and allow the customer to have a satisfying experience. We want to make ourselves available at all times with the utmost greetings. This became a challenge at first when we weren't able to see and help our customers. However, we figured it out. We were able to still give the same great customer service with the help of current day technology.

Covid-19 had left huge impression on the world, good and bad. Security and fraud was a big part of that impression. Fraudster still needed to make a living so they found new ways to do so. In my personal experience in my career of 10 years in banking, I have dealt with more fraud in the past three then ever before. Most due to the use of online shopping. Merchants data would be compromised due to the lack of upgrades and being more susceptible. This was one of the main reasons a push for the tap-to-pay chip cards. It would eliminate confidential data from the transactions. Some consumers during the time of the pandemic were also financially struggling, this made them more susceptible to fraud. Bankers, including myself were having to communicate with customers what to be aware of in order to protect their money.

Covid-19 also helped reshape what we knew as the 9 to 5. Employees now have the ability to work from home with less hours with the help of advanced technology. I saw this first hand working at my financial institution. Our office staff was divided into different groups in order to ensure there was a functioning staff available at all times to run the location. With the help of the advanced technology both groups were able to maintain communication and continue with work production in a safe environment.

This opened the doors for companies to realized they can offer positions that are work from home based. Individuals now in present day search for jobs that allow them to work from home full time. This gives them the ability to be more present at home all while maintaining a career and earning a living.

Security of all counts also plays a role with technology. Security is vital for a financial institution to operate and of course protect customer's confidential information. Today financial institutions do not hold the same physical amount of cash they used to but the need to physical security is still needed. However, billions of dollars are accessible and without proper security in place hackable.

To help gain that trust for the next generation financial institutions need to protect the customer's financial data securely. By investing in the technology for better monitoring and control system this can safeguard customer and their information.

Technology has even reshaped the way financial institutions market their brand. In monthly marketing meetings we are always discussing the best way to advertise and get our messages out to the public. It is drastically different than 20 years ago. Social media is the main show in 2022 and is too valuable of an opportunity to not avoid. Companies and their leaders need to make the choice if they haven't already and get their institution socially connected.

Alongside being connected the option for cross-selling is massive. We are now able to use data to better understand our customers. We can deliver content that is wanted and personalized. We are able to keep customers engaged and cross-sell products that will actually benefit them as a consumer.

In today's time customers truly have all the power. In the long run their decision on where to look for their next financial need to be met by the products the financial institution can

offer them. Financial institutions who evolve and innovate their technology and products to fit have everything to gain.

Essentially being a banker, we help guide our customers through how to manage family finances, healthcare spending, retirement savings, online shopping, e-banking, as well as learning how to use evolving technology. I have helped countless customers of all ages manage their accounts, plan out budgets and set up accounts digitally. Over that time, I have seen how our everyday lives have changed due to technological enhancements. Consumers who had to manage finances in the late 1990's are not having to manage the same criteria as they are in the current day.

References

Bush, V. (1997). The role of technology. *America's Community Banker, 6*(10), 37-p45.

Chung, Schuettel & Struebi. (2022). The art of courting wealthy millennials. *ABA Banking Journal.* Retrieved on November 1, 2022 from https://bankingjournal.aba.com/2022/04/the-art-of-courting-wealthy-millennials/

Conant, B, & Harley, N. (2022). Bank tech trends for 2022. *ABA Banking Journal*. Retrieved on April 1, 2022 from https://bankingjournal.aba.com/2022/01/bank-tech-trends-for-2022/

Colgan, C. (2020). Human customer service in the digital age: The challenge to adapt. *ABA Banking Journal, Volume* (Issue), 39-41.

Daniels, L. (2021). Four best practices for advancing bank cybersecurity programs for the cloud age, *ABA Banking Journal*. Retrieved on April 3, 2022 from https://bankingjournal.aba.com/2021/12/four-best-practices-for-advancing-bank-cybersecurity-programs-for-the-cloud-age/

Dixon, M. (1999). 39 experts predict the future. *America's Community Banker, 8*(7), 20-p31.

Farley, A. (2015). Focus on social media engagement. *ABA Banking Journal*. Retrieved on October 31, 2022 from https://bankingjournal.aba.com/2015/03/with-social-media-focus-on-your-fans-engagement-level/

Gibson, M. (2022). ABA survey: Three trends driving change in bank marketing. *ABA Bank Marketing.* Retrieved on November 1, 2022 from https://bankingjournal.aba.com/2022/07/aba-survey-three-trends-driving-change-in-bank-marketing/

Gross, E. (2021). Ensuring the security of the digital banking experience. *ABA Banking Journal.* Retrieved on April 2, 2022 from https://bankingjournal.aba.com/2021/03/ensuring-the-security-of-the-digital-banking-experience/

Hintze, J. (2022). Tailoring hybrid and remote work key to attracting and retaining talent. *ABA Banking Journal*. Retrieved on October 30, 2022 from https://bankingjournal.aba.com/2022/09/tailoring-hybrid-and-remote-work-key-to-attracting-and-retaining-talent/

Hoffman, K. (2020). Emerging vectors for payment fraud. *ABA Banking Journal.* Retrieved on April 2, 2022 from https://bankingjournal.aba.com/2020/04/emerging-vectors-for-payments-fraud/

Hoffman, K. (2020). Securing the remote bank workforce. *ABA Banking Journal.* Retrieved on April 3, 2022 from https://bankingjournal.aba.com/2020/05/securing-the-remote-bank-workforce/

Knudson, J. (2022). Top bank risks for 2022. *ABA Banking Journal.* Retrieved on April 1, 2022 from https://bankingjournal.aba.com/2022/01/top-bank-risks-for-2022/

Meinert, M. (2018). Payment trends to watch in 2019. *ABA Banking Journal.* Retrieved on April 2, 2022 from https://bankingjournal.aba.com/2018/11/payments-trends-to-watch-in-2019/

Meinert, M. (2020). A return to (more or less) normal bank operations. *ABA Banking Journal.* Retrieved on April 2, 2022 from https://bankingjournal.aba.com/2020/05/a-return-to-more-or-less-normal-_bank-operations/

Morgan, R. (2020). The future of the branch in a digital world. *ABA Banking Journal.* Retrieved on April 4, 2022 from https://bankingjournal.aba.com/2020/06/the-future-of-the-branch-in-a-digital-world/

Oberly, D. (2022). What banks need to know about new data breach notification requirements. *ABA Banking Journal.* Retrieved on April 3, 2022 from https://bankingjournal.aba.com/2022/02/what-banks-need-to-know-about-new-data-breach-notification-requirements/

Oxford, J. (2020). Still the best way to connect. *ABA Banking Journal*. Retrieved April 3, 2022 from https://bankingjournal.aba.com/2020/05/still-the-best-way-to-connect/

Pulusani, P (2022). Digital strategies to show boomer they matter. *ABA Bank Marketing*. Retrieved November 1, 2022 from https://bankingjournal.aba.com/2022/07/digital-strategies-to-show-boomers-they-matter/

Ren, H. (2019). Social media that matters. *ABA Banking Journal.* Retrieved April 3, 2022 from https://bankingjournal.aba.com/2019/09/social-media-that-matters/

Riccio, T. (2020). Using technology to improve health and safety in the branch. *ABA Banking Journal.* Retrieved on April 3, 2022 from https://bankingjournal.aba.com/2020/09/using-technology-to-improve-health-and- safety-in-the-branch/

Vergara, D. (2020). Four tips for securing digital banking channels. *ABA Banking Journal.* Retrieved on April 2, 2022 from https://bankingjournal.aba.com/2020/11/four-tips-for-securing-digital-banking-channels/

Westby, M. and Wolf, L. (2019). What compliance needs to know in the event of a security breach. *ABA Banking Journal.* Retrieved April 2, 2022 from https://bankingjournal.aba.com/2019/09/ what-compliance-needs-to-know-in-the-event-of-a-security-breach/

Whitcomb, D. (2022). Banking for Z next generation. *ABA Banking Journal.* Retrieved on November 1, 2022 from https://bankingjournal.aba.com/2022/06/banking-for-z-next-generation/

Wilber, D. (2020). Three ways bank CEOs can lead the social media charge. *ABA Banking Journal*. Retrieved on April 2, 2022 from https://bankingjournal.aba.com/2020/04/three-ways-bank-ceos-can-lead-the-social-media-charge/

Wilber, D. (2022). How social media data improves cross-selling for banks. *ABA Banking Journal*. Retrieved on October 31, 2022 from https://bankingjournal.aba.com/2022/04/how-social-media-data-improves-cross-selling-for-banks/