Innovation, insight and trust: Customer experience excellence delivered responsibly in a digital world

Received (in revised form): 20th November, 2019

Mike Heffner
Global Industry Lead, Appian, USA

Mike Heffner leads the Global Industry group at Appian. The team is responsible for engaging with customers, partners and analysts to solve digital transformation challenges in all important verticals, including the public sector, life sciences, health care, energy, insurance, banking, and capital markets. Mike brings innovative approaches to problem-solving to his role, including extensive leadership experience in operational efficiency and business transformation. He is a speaker, author and thought leader on digital trends and responses. Prior to Appian, he was Managing Director, Business Transformation, at State Street Corporation and held management roles at Charles Schwab & Co. and Accenture's Creating-Financial-Markets-Advantage executive group. Mike holds a Bachelor of Science in Business Administration (BSBA) in Economics from the University of South Carolina and an MBA from Babson College.

Global Industry Leads, Appian, 7950 Jones Branch Dr, Tysons, VA 22102 USA
E-mail: michael.heffner@appian.com

Guy Mettrick
Industry Leader for Financial Services in EMEA, Appian, UK

Guy Mettrick is Appian's Industry Leader for Financial Services in Europe, Middle East and Africa (EMEA). He is responsible for driving Appian's go-to-market strategy for Financial Services across the region. The role includes working with customers, partners and industry associations to ensure Appian deliver solutions that help drive growth, manage risk and increase the efficiency and effectiveness of their business processes. Previously, he was Head of European Fund Business at Sumitomo Mitsui Trust Bank. He has also held management positions at BNP Paribas and RBC. Guy has a Bachelor of Arts degree in Business Studies (Finance & Marketing) from the University of Portsmouth.

Financial Services, Appian 24 Martin Lane, London, EC4R 0DR
Tel: +44 20 3861 6298
E-mail: guy.mettrick@appian.com

Abstract Financial institutions are investing in innovative solutions that help restore customer trust — an imperative focus amid high-profile data breaches and post-financial crisis apprehension. Many have made data privacy central to their day-to-day operations, recognising its importance as a competitive differentiator. Financial institutions, however, face the added challenge of dedicating the necessary attention to improving the customer experience, achieving regulatory compliance and maintaining robust security. This paper covers the capabilities and benefits of a low-code automation platform, a scalable solution that supports financial institutions in putting the customer first. Low-code dramatically simplifies the process of building and deploying applications while reducing the time it takes to do so. It empowers citizen developers with the ability to bring their ideas to life with intuitive point-and-click methods, replacing manual and redundant lines of code. Finally, low-code applications have the ability to store data on one interface, promising a single source of truth and providing employees with the right information at the right time. Supported by rigorous security standards and compliance,

low-code delivers the security customers demand of financial institutions, ensuring that personal and financial data is safe. Essentially, low-code allows business and IT to work together, aligning their priorities towards one goal: making the customer successful.

KEYWORDS: trust, customer experience, technology, innovation, low-code, privacy, security, customer data

According to a 2016 Gallup poll, just 27 per cent of adult Americans have confidence in banks.[1] That is a sizeable decrease since 2004, when 53 per cent expressed confidence. Meanwhile, post-financial crisis customer trust continues to wane with the proliferation of high-profile data breach incidents. Nearly two-thirds (60 per cent) of global consumers surveyed by Ernst & Young (EY) said they worry about their bank accounts or bank cards being hacked, and 59 per cent said they worry about the personal information public and private sector organisations have about them.[2]

New solutions are needed to restore trust, requiring an investment in innovative solutions that empower financial institutions to stay ahead of emerging threats and leverage historical data in their efforts to strengthen security and compliance. Financial institutions must make it a priority to reassure customers of their data protection and privacy at every stage of the customer journey, further improving the customer experience (CX).

When we talk about 'innovation in finance', most people immediately think of FinTech — the cool, cutting-edge start-ups that are leading the sector in digital transformation with new business models and technologies designed to engage customers.

Many financial institutions struggle to keep up because they are encumbered by legacy systems and (necessarily) laser-focused on regulatory compliance. They realise they are at risk of letting the innovation train pass them by and that this is a perilous situation for their business. Still, they do not know how to get on the train except through painful and costly technology infrastructure rip-and-replace, using time and resources they do not have to start again from scratch.

The good news: today's financial institutions no longer have to choose between innovation, compliance and trust. A low-code automation platform can enable all three.

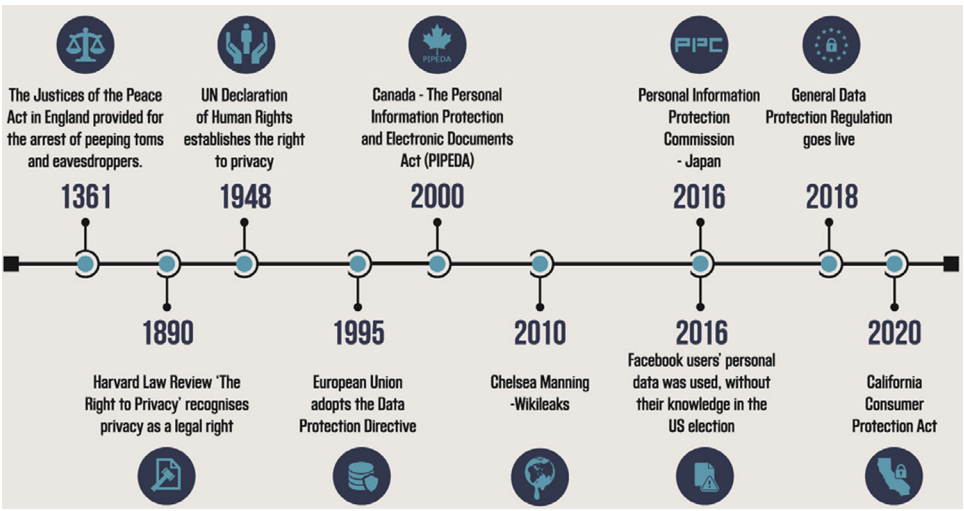

Figure 1: The History of Privacy, Appian Corporation, 2019

THE HISTORY OF PRIVACY

The protection of a person's private information became a concern long before today's era of cyberattacks, nation-state actors and data breaches. In 1361, the Justices of the Peace in England gave communities the right to arrest eavesdroppers and 'peeping Toms'. Fast-forward to Warren and Brandeis' 'The Right to Privacy' paper, published in the 1890 *Harvard Law Review*. It is widely regarded as the first publication in the United States to advocate for a right to privacy.

Progress accelerated in the 20th century. After World War II, the United Nations established the right to privacy in the UN Declaration of Human Rights. In the decades that followed, the adoption of the computer, and then the Internet, made consumer information available to an unprecedented degree. Addresses, bank account balances, national identification numbers (such as Taxpayer Identification and Social Security numbers) and more were now stored in files that could be shared — first by disc, then via e-mail — across companies and the world.

In 1995, the European Union responded with the Data Protection Directive, which regulates how data is collected and processed within the EU. Its seven principles — notice, purpose, consent, security, disclosure, access and accountability — would later inform the General Data Protection Requirement (GDPR), now governing all parties that handle the data of EU citizens. In 2000, Canada enacted its own privacy regulations, the Personal Information Protection and Electronic Documents Act (PIPEDA).

Then came the United States' financial crisis of 2008 followed by the Great Recession: The S&P plummeted, and millions lost their homes, jobs or both. 'For many, faith in homeownership, the financial markets and a government-provided security net never quite felt secure again', an article in the *Chicago Tribune* declared.[3] Public trust in banks fell from 53 per cent in 2004 to a low of 21 per cent in 2012.[4] People became concerned about the way financial institutions handled both their money and their personal data.

In the 2010s, data privacy and security issues escalated to become global threats of unprecedented proportion and impact. The decade that kicked off with WikiLeaks shows no signs of slowing: in 2016, the public learned that Cambridge Analytica had bought Facebook data on tens of millions of Americans without their knowledge. In the words of *Wired* magazine, Cambridge Analytica 'sparked the great privacy awakening'.[5]

Along with GDPR's institution in 2018, other nations around the world have also strengthened their own data privacy environments. For example, Japan created the Personal Information Protection Commission to enhance its system of privacy laws and amended its regulations on the protection of personal information to apply to both foreign and domestic companies that process the data of Japanese citizens.[6,7]

As we approach the next decade, US states are taking privacy into their own hands as well. The California Consumer Privacy Act applies to any business that has more than $25m in revenue, buys or sells the personal information of 50,000 or more consumers, or derives 50 per cent or more of its annual revenue from selling consumers' personal information, and does any amount of business in the state of California. The Act will come into effect in 2020, giving consumers rights including:

- The right to know *all* information a business collects about them
- The right to say no to the sale of their information
- The right to sue a company that collected their data and then had this data stolen or compromised in a breach
- The right to delete data they have posted[8]

Financial institutions that fail to learn from history are doomed to repeat it. Data privacy

is no longer a back-office activity completed for the sake of compliance. It is a priority that, when handled poorly, can impact a financial institution's reputation, return on investment (ROI), safety and bottom line. Customers are making buying decisions on the basis of who takes care of their information best because they have seen the consequences of those who do not. Gemalto, an Amsterdam-based digital security firm, conducted a survey and reported that 59 per cent of respondents said they would stop using a bank if it experienced an online breach.[9] A study by March Networks found that one in five US customers say they have changed banks owing to a negative customer service experience.[10]

PRIVACY AS A COMPETITIVE DIFFERENTIATOR

Most US consumers, particularly millennials, are considered 'data pragmatists', meaning they will trade personal information for certain incentives or benefits.[11] This gives financial institutions great opportunities to gather information about individuals, then leverage the information to provide a more personalised financial experience. As the Gemalto survey reveals, however, when banking customers feel as though their personal information is being mistreated or unprotected, they will likely seek business elsewhere.

Financial institutions have no choice but to heed this warning, and they are responding by going to great lengths to protect their customers' information. According to Forrester, the application security market will exceed $7bn by 2023.[12] The next step, however, is making data privacy central to your financial institution's day-to-day operations — and its marketing message. Given that only 25 per cent of consumers believe most companies handle their sensitive personal data responsibly,[13] differentiating on privacy and trust is a great business opportunity.

Strengthening trust with customers is an important ingredient in acquisition and retainment. What else increases customer loyalty? The convenience of modern-day banking. Robo-advisor tools, mobile banking, peer-to-peer payment apps and so on have largely contributed to lower levels of bank customer churn.[14] In 2018, only 4 per cent of customers switched banks — the lowest number of switching ever recorded.[15]

Achieving both trust and convenience depends on choosing the right technology partner. Technology is crucial to organising data, keeping it secure and optimising the customer experience with interactions that put people at the centre.

RISKS OF A NON-SUSTAINABLE PRIVACY APPROACH

Any discussion of data privacy calls for a deep understanding of a financial institution's entire data life cycle. It is important to track data through an organisation by capturing what processes control data, who has access to data and where data is stored. Knowing the controls around customer data is essential for financial institutions to deliver personalised customer interactions that drive their competitive edge while also remaining compliant with data privacy regulations.

Unfortunately, established financial institutions are challenged by the many legacy systems built through the years that store and manage this data. A timely example is the upcoming retirement of LIBOR in 2021. This looming deadline is forcing financial institutions to repaper and renegotiate trillions of dollars' worth of US financial contracts. This will require financial institutions to review all existing credit agreements and contracts and then determine the right path forward. Finance, legal and operations teams tasked with the job of scrutinising these contracts to find, assess and remediate all LIBOR instances will find it nearly impossible to do manually.

LIBOR is just one example. The changes associated with Brexit, along with regulations around initial margin, will require financial

institutions to scrutinise their client and trade contracts. If done manually, or as a one-off data cleansing exercise, the results will be costly, time-consuming and ultimately ineffective. Inefficient, people-driven data management results in passive monitoring, excessive time and effort training employees on manual procedures, and lost tribal knowledge—and data integrity—during staff turnover and other transitions. Any manual data entry increases the risk of human error, which can negatively affect customer experience — a major predictor of business growth. In the Financial Services industry, healthy client relationships translate into customer retention, providing the staying power and renewed marketability to continue to acquire new customers. Happy (and unhappy) clients directly impact the bottom line.

Siloed operations present another challenge. Data that is misaligned across business functions and geographies stifles natural organisation changes and evolution. And if financial institutions struggle to maintain useful data, how can they collaborate? How can they fully understand their customers and provide the personal experiences the marketplace demands?

To address these data management challenges, financial institutions typically take one of four routes: start from scratch, stack legacy architecture, do nothing or implement a flexible software solution.

Here is a breakdown of each.

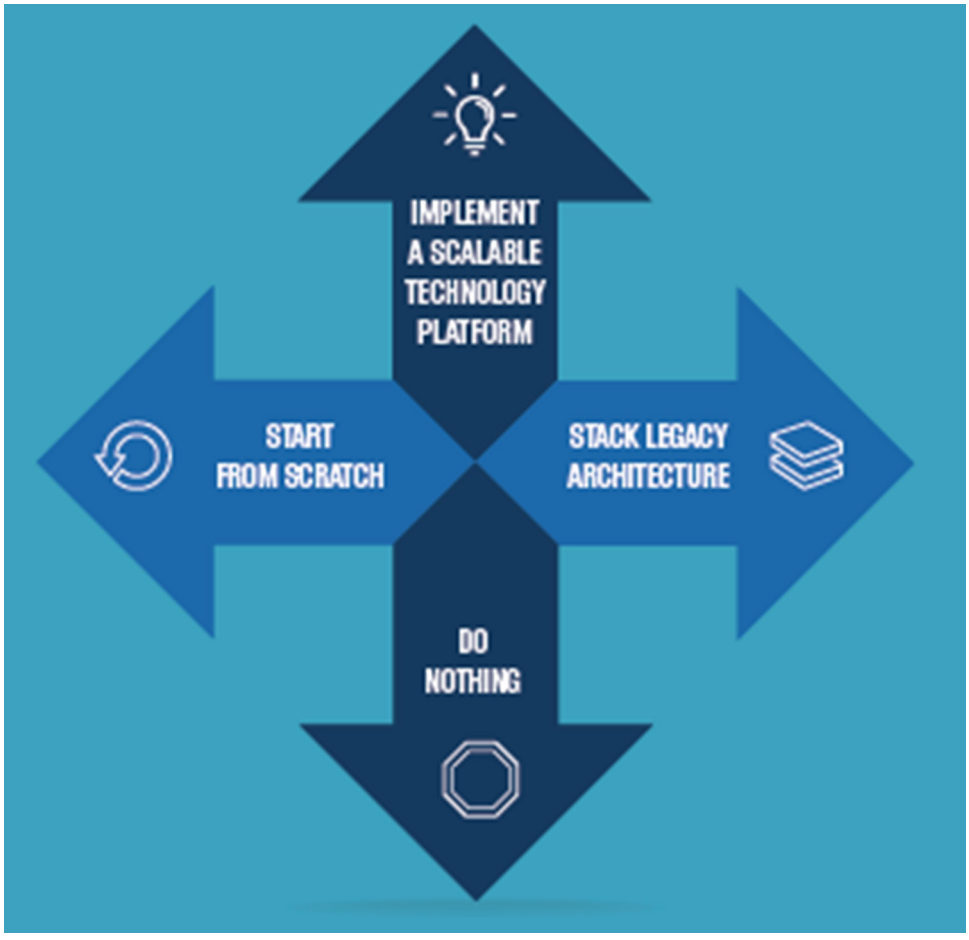

Figure 2: Four Routes to Digital Transformation, Appian Corporation, 2019

Option 1: Build a new greenfield architecture

Building or buying a brand new software solution for architecture and data can be a clean option that ultimately leads to faster processes. The time and resource investment required to start from scratch, however, could be substantial. And with a new system, there can be challenges relating to legacy data and ensuring the best path forward without sacrificing history and important customer data.

Furthermore, the planning and implementation processes for a new software solution present an array of potential issues. Stakeholder input will need to be collected from across the organisation, which can result in conflicting opinions and priorities. This will have to be followed by identification of the staff responsible for keeping things moving, setting goals, establishing metrics for reaching those goals and so on.

Who will transfer all the data? Who will initiate training? These challenges can easily overwhelm employees already juggling a full workload, leading to missteps along the road towards digital transformation success.

Option 2: Stack legacy infrastructure

Point solutions and legacy architecture burden financial institutions from an efficiency standpoint, with detrimental effects on customer satisfaction. But many do not consider the gaps in vulnerability when it comes to legacy systems. Their rigid structure makes it difficult for users to alter processes as new needs and opportunities arise, and legacy systems simultaneously make it easy for adversaries to infiltrate and access valuable data.

Many financial institutions implement multiple point systems looking for cost savings or aiming to reinforce security and capabilities. Legacy systems tend to have very specific functionality, and small updates often result in multiple conflicts across the system. Faced with these challenges, stacking point solutions on top of legacy infrastructure may seem like an alternative way to fulfil all processes and offer customers the experience they demand while simultaneously avoiding expensive updates.

When you are working with legacy systems and multiple point solutions, however, data accuracy deteriorates. It is stored in silos with multiple people relying on different sources of truth, resulting in misaligned priorities as well as privacy concerns — both of which can negatively impact customer trust and loyalty.

Stacking legacy systems makes financial institutions, and customers' personal information, vulnerable. After all, the more places data lives, the more opportunities it presents for a malicious actor to get his or her hands on it. In addition, without an accurate source of customer information, customer service agents may ask for information that was already provided. Customers look for speed and convenience, and engaging them in repetitive tasks is no way to achieve an exceptional customer experience.

Stacking legacy infrastructure presents internal headaches as well. If customer information is in one system, product information in another and company and departmental information in yet another, agents have to perform 'swivel chair' integration as they go from screen to screen or system to system. They are often required to copy and paste information from one system to another, lack a unified data and spend time manually rekeying information. This slows agent response, increases the risk of human error and lessens job satisfaction for the agent. Financial institutions can also face talent gaps and high training costs as they struggle to hire and train people on how to use each system.

Beyond the impact on employees, this error-prone, slow approach negatively impacts the customer experience. Given customers'

concerns about privacy, financial institutions cannot afford a breach. They need to be able to assure customers their information is safe, and it is hard to make that promise when data is stored across multiple legacy systems. Armed with accurate, insightful customer data that is stored safely in a unified system, financial institutions can give customers the individualised approach they are looking for while assuring them their information is in the right hands.

This is especially crucial given that financial institutions lost significant customer trust during the 2008 crisis. Since then, they have sought ways to earn it back and keep up with trends in technology simultaneously. Many have looked for solutions that help them achieve both. After all, it is about more than avoiding a breach. It is about knowing your customer and using organised, protected data to improve the customer experience.

Option 3: Implement a secure, scalable automation platform

How can financial institutions innovate and deliver engaging, memorable customer experiences while complying with changing regulations and requirements? A low-code automation platform is the answer.

Low-code is a new approach that replaces specialised coding with a visual drag-and-drop method of application development. It allows business users to create intuitive applications by drawing the picture like a flow chart, instead of writing lines of code.

How? Low-code application platforms provide:

- A rapid way to programmatically define business process, getting business requirements into code rapidly
- Seamless integrations — the ability to bring in modern API calls as well as support for legacy authentication and integration
- A powerful user interface (UI) framework that a workforce intuitively understands, giving them the ability to access the resources they need and providing an experience that is a joy to use
- Compliance with governance controls and security, table stakes in a highly regulated industry

This drastically reduces the time required to build, deploy and change enterprise applications in a competitive, fast-paced environment. Low-code allows business and IT to work together, lending the power and flexibility to automate tasks, organise data and keep customer information safe. Even more, it delivers all of this up to 20 times faster than traditional coding.

Low-code's visual modelling makes it easy to bring their application ideas and needs to life. And every object — fact, interface, integration — is reusable to further streamline the process. You can implement declarative tools through visual models and business rules, eliminating the need for custom coding and making difficult changes in the future. Other features of low-code include instant mobility, making cross-platform functionality a standard part of design. With no extra effort, coding or resources, your customers can access the information they need on any device — mobile, tablet or desktop.

CASE STUDY: LOW-CODE FOR ONBOARDING

When a major bank underwent the process of implementing low-code applications for onboarding, it framed its approach through a business perspective. Essentially, it put the customer at the centre of everything it did — exactly the mentality that low-code was created for.

The bank wanted to avoid the common challenge of collecting information about customers and keeping it in separate

applications. It also wanted to make sure the customer did not have to answer the same question multiple times and the employee did not have to input the same data multiple times. Repetitive tasks like these waste precious hours, contribute to inaccuracy and inefficiency and degrade customer and employee experience.

Using Appian's low-code application, the bank implemented a four-step process, consisting of prospecting, client onboarding, product onboarding and servicing. Through each step of the process, the bank was absorbing a lot of information about customers, then using it to better understand risk and opportunity. Low-code also supported the bank to use the same process for every product — whether a customer was inquiring about a savings account, mortgage or small business loan.

Employees at the bank were able to access the information they needed when they needed it, thanks to low-code's ability to filter relevant data through complex business rules and processes. Further, the bank complied with regulations and adhered to security standards while maintaining a scalable application that can change as the enterprise changes.

COMBINING TECHNOLOGY WITH THE HUMAN TOUCH

Building an application on a low-code automation platform extends your financial institution's capabilities across applications and processes: new business, lending, the customer's journey, along with governance, risk and compliance. Using low-code for dynamic case management applications, for example, allows you to gain visibility, fast-track workflows and empower knowledge workers throughout the enterprise. Essentially, it is a way to reach desired business goals by maximising both structured processes and human intuition.

Intelligent automation is an important component that supports organisations in building customer trust. It is the combination of business process management (BPM), artificial intelligence/machine learning (AI/ML) and robotic process automation (RPA). In relation to low-code, intelligent automation enables cohesive process and data orchestration across humans, smart machines and robots. This empowers financial institutions to clean, organise and update data in real time, increasing efficiency without sacrificing accuracy. And when all these emerging technologies exist on a low-code automation platform, they are no longer exclusive to the ivory towers of data scientists. Business and IT resources are maximised, freeing teams to spend more time improving the customer experience and building trust.

With accurate data, financial institutions can also equip call centre agents with the information they need to give customers a fast, stress-free experience. Rather than wait on hold, customers are greeted by a human or an intelligent robot, equipped with all their pertinent data, from their address to their purchase history. This dramatically streamlines any interactions with customers and increases their trust in your financial institution. Of course, the most significant way to deliver value here is to cohesively orchestrate omnichannel customer communications across the human and robotic workforce — something that low-code platforms can do very well.

With low-code, it is not necessary for financial institutions to move all their data onto a new system. Low-code has the ability to unite legacy systems, seamlessly integrate data and allow for business process and collaboration management. You can also build applications that natively run on both mobile and Web, with trusted security, reliability and governance. And you have the flexibility to host these applications anywhere: in the cloud, on-premise or hybrid environments.

Low-code is a promising option for financial institutions that want to innovate without compromising compliance and trust. It allows organisations to unify historical processes and data while maximising security,

efficiency, productivity — all variables that contribute to a positive customer experience and strengthened customer trust.

HOW ACCURATE DATA AND A LOW-CODE AUTOMATION PLATFORM TRANSLATE TO BETTER CX

A low-code automation platform with dynamic case management capabilities does more than streamline back-end operations. It creates a convenient, engaging experience for your customers and your customer's customers — which will, in turn, increase their trust in and loyalty to your financial institution. For this reason alone, if CX improvements are not on the top of your priority list, they should be. According to Forrester, the revenue impact of a one-point improvement in CX index scores can yield $19bn more assets under management for the average multichannel brokerage and $6bn more assets for the average direct brokerage.[16]

The challenge that financial institutions confront has much to do with how they are turning troves of data into actionable insight. 'Machine learning is becoming ubiquitous, but organisations are struggling to turn data into value', McKinsey wrote in its report 'Analytics Comes of Age'. 'By identifying, sizing, prioritising, and phasing all applicable use cases, businesses can create an analytics strategy that generates value'.[17]

While low-code applications can provide a 360-degree view of the customer, many employees within financial institutions do not need full details about every individual with whom they are interacting. Low-code stores troves of data within one interface but presents relevant information to relevant parties at the right time. This structured visibility also increases security, since the entire enterprise does not have access to every detail about every customer.

Traditional approaches to privacy started with data, followed by technology and processes and, finally, people. But the way we use data today calls for a people-first approach, one that is fast and intuitive and that allows people to visualise the solution — the business logic, interfaces, rules, integrations and all the other components — and then translates it instantly into working software. That is how low-code works.

Low-code solutions drastically ease the process of generating value from data. They unify legacy systems and processes, ensuring you have an accurate view of customers — where they began their journey with your organisation, how their financial needs and goals have changed and everything in between. This also includes their preferences, including how they interact with your financial institution. With this knowledge, you can more swiftly and effectively anticipate, identify and respond to their evolving demands.

Here is how low-code software helps financial institutions put their customers first:

Business alignment. Privacy can be a differentiator. Customers choose to do business with the financial institution that better understands them and takes better care of their information. In a Harris poll surveying 2,000 people, 65 per cent of respondents said data privacy was the issue they wanted companies to address most.[18] Therefore, deploying robust security measures does more than protect data. It strengthens your institution's competitiveness in the marketplace by addressing the needs of your customers. Low-code applications support overall business alignment by granting visibility over processes. The more teams understand each other's workflows, the more they can optimise collaboration and work towards the same goal: making the customer successful.

Future-focused collaboration. To succeed in today's environment, organisations need technology that supports work across the enterprise and evolves with changing conditions. Financial institutions, in particular,

Figure 3: How Low-code Helps, Appian Corporation, 2019

require reusable components they can repurpose for different lines of business. The larger the business, the more difficult it becomes to break down walls. Typically, in large firms teams are working in different lines of business, making decisions on the basis of siloed data and struggling to communicate with other departments. Low-code solutions break down those walls, offering the visibility to transcend those boundaries and adapt to whatever comes next. Individuals across the enterprise can see the status of any process, set notifications and alerts to keep momentum going and identify any progress inhibitors.

Global personalisation. Financial institutions serving customers worldwide at all stages of the client life cycle are challenged to deliver personal, localised experiences without losing anything in translation. Low-code solutions enable financial institutions to implement powerful solutions in multiple geographies, while quickly adapting to different currencies, languages, regulations and other jurisdiction-specific variables. Using global templates, organisations can achieve global business diversity and business unit autonomy with integrated tools that are reusable and scalable. Carefully considered business process models act as a business blueprint, adaptable for roles and authorisations, controls and compliance frameworks. When delivered with beautiful interfaces and powerful integrations, it all comes together to provide exceptional user experience.

Flexibility and customisability. Customised processes are possible — and send positive ripple effects through the

business. Low-code solutions empower your teams with customised workflows and other smaller-scale customisations that make sense for your needs and your customers' needs. What is more, departments will be able to operate autonomously, even if they are sharing data across various lines of business. The central purpose of low-code is to provide users with the flexibility to make the software work for them — not change their operations according to the software's rigid structure. When you have control over processes and data, you can bring ideas to life and give customers a stellar experience.

Simple integration. In the era of 'big data', the goal should not be about simply collecting as much information as possible. Organisations need to draw pertinent patterns and insight from these troves. When data lives in separate areas of a business, however, this process can become long and arduous and leave room for error. A flexible, low-code automation platform unifies this data, including the data you acquire from third parties, for easy access. Once the data is in order it becomes easier to realise the vision of new products, services and features, helping you further simplify your processes, streamline transactions and make confident decisions.

To save time and effort, look for a low-code automation platform that:

- Allows you to leave your data where it is — on premise or in the cloud
- Has trusted security, reliability and governance
- Provides the ability to integrate data across existing systems

State-of-the-art security. Given the sensitive information financial institutions collect and store, attackers are becoming more adept and better equipped, and data breaches have become commonplace. In 2018, data breaches and cyberattacks affected billions of people — 765 million through April, May and June alone.[19]

Whatever the motivation of these criminals — to monetise stolen data in flourishing underground markets, to keep the data for their own espionage purposes or to use stolen funds to facilitate future operations — financial institutions are struggling to innovate and improve the customer experience while simultaneously focusing on security and privacy.

Organisations often stack legacy infrastructure in their vain attempts to do so, but they are essentially creating wider gaps for nefarious activity to penetrate its walls. Security should be the chief priority for your software vendor, aligning with leading National Institute of Standards and Technology (NIST), Payment Card Industry Data Security Standard (PCI DSS) and other frameworks. Forward-thinking technology partners should support hybrid cloud architectures to allow customers to leverage some aspects of a cloud platform while also leveraging on-premise components to form a complete solution. Hybrid cloud offerings allow complete control over data and ensure data privacy for both security and governmental compliance purposes.

Threats are only becoming more sophisticated, so financial institutions are wise to not only anticipate changes in customer demands or market trends, but also to think about the future of hacking. Strengthen security by partnering with a vendor that stays ahead of hackers and threats. This vendor should hold up-to-date and relevant security certifications, undergo frequent third-party audits, proactively monitor network activities and anticipate market trends and customer demands — all essential steps in keeping your business and your customers' data safe.

LOW-CODE AND THE POWER OF ARTIFICIAL INTELLIGENCE

Artificial Intelligence (AI) is essential to making your applications smarter. Low-code is designed to support AI, resulting in a fast,

simple decision-making process. Financial institutions can integrate AI services on their low-code automation platform to gain insights that further improve business outcomes.

AI can be scaled according to a financial institution's growth, allowing you to see real impact immediately. It is all about meeting customers where they are and establishing trust early on.

With the right mix of humans and robots working together, financial institutions have the intelligence to apply context to data, flag risks and identify patterns — all supporting your pursuit to improve CX safely and securely.

CONCLUSION

Financial institutions must prioritise strengthening trust with customers and cultivating trusted brands as a way to differentiate themselves from both new and existing competitors. Trust is essential for growing a loyal customer base and is a predictor of advocacy and future business.

Loyalty grows from serving customers with simpler processes and personalised experiences that respond to financial needs in real time. This level of customer service excellence and deep personalisation requires large volumes of data. But with great data access comes great responsibility. To be transparent and accountable to the customers they serve, financial institutions must balance the customer experience with data privacy.

Complicated processes, disjointed accounts and legacy technology can make such transparency, accountability and trust difficult to achieve. To overcome this challenge, financial institutions must think of data privacy as a competitive differentiator that improves the customer experience, not as a back-office activity for compliance. They also need the power of low-code applications that let them identify, link and reconcile data from various sources for a unified and trusted customer view — with the flexibility to evolve with business growth and changing regulations.

Low-code is the answer to making a financial institution's job easier while making the customer experience outstanding. It eliminates the cumbersome tasks often required to undergo a digital transformation, empowering business and IT teams to build effective applications fast. And it allows you to confidently tell your customers their data is safe, accurate and being used responsibly.

References

1. McCarthy, J. (2016) 'Americans' confidence in banks still languishing below 30%', *GALLUP*, available at https://news.gallup.com/poll/192719/americans-confidence-banks-languishing-below.aspx (accessed 23rd August, 2019).
2. Ernst & Young. (2016) 'Customer trust: Without it, you're just another bank', available at https://www.ey.com/Publication/vwLUAssets/ey-trust-without-it-youre-just-another-bank/$FILE/ey-trust-without-it-youre-just-another-bank.pdf (accessed 31st July, 2019).
3. Associated Press. (2018) 'One decade after the financial crisis, here's how the financial system has changed', *Chicago Tribune*, available at https://www.chicagotribune.com/business/ct-biz-anniversary-financial-system-20180913-story.html (accessed 16th August, 2019).
4. Ibid.
5. Lapowsky, I. (2019) 'How Cambridge Analytica sparked the great privacy awakening', *Wired*, available at https://www.wired.com/story/cambridge-analytica-facebook-privacy-awakening/ (accessed 9th August, 2019).
6. Takase, K. (2017) 'GDPR matchup: Japan's act on the protection of personal information', *International Association of Privacy Professionals*, available at https://iapp.org/news/a/gdpr-matchup-japans-act-on-the-protection-of-personal-information/ (accessed 9th August, 2019).
7. Simmons, D. (2019) '6 Countries with GDPR-like data privacy laws', *Comforte AG*, available at https://insights.comforte.com/6-countries-with-gdpr-like-data-privacy-laws (accessed 9th August, 2019).
8. Californians for Consumer Privacy. (n.d.) 'About the California Consumer Privacy Act', available at https://www.caprivacy.org/about (accessed 9th August, 2019).
9. Urrico, R. (2017) '70% of consumers would stop following a business after a data breach', *Credit Union Times*, available at https://www.cutimes.com/2017/11/29/70-of-consumers-would-stop-following-a-business-af/ (accessed 12th August, 2019).
10. Sullivan, A. (2017) 'Poor service and security issues driving consumers to switch banking providers', *The Financial Brand*, available at https://thefinancialbrand.com/68426/banking-customer-service-security-branch/ (accessed 12th August, 2019).

11. Acxiom. (2018) 'Data privacy: What the consumer really thinks', available at https://marketing.acxiom.com/rs/982-LRE-196/images/DMA-REP-DataPrivacy-US.pdf (accessed 12th August, 2019).
12. Forrester. (2018) 'Application security market will exceed $7 billion by 2023', available at https://www.forrester.com/report/Application+Security+Market+Will+Exceed+7+Billion+By+2023/-/E-RES144054# (accessed 5th August, 2019).
13. Pwc. (2017) 'Consumer intelligence series: Protect.me', available at https://www.pwc.com/us/en/advisory-services/publications/consumer-intelligence-series/protect-me/cis-protect-me-findings.pdf (accessed 22nd August, 2019).
14. Shevlin, R. (2019) 'Why people don't switch banks anymore', *Forbes*, available at https://www.forbes.com/sites/ronshevlin/2019/05/01/why-are-fewer-consumers-switching-banks-because-checking-accounts-have-become-paycheck-motels/#4457ac232aa9 (accessed on 21st August, 2019).
15. Ibid.
16. McKinsey Analytics. (2018) 'Analytics comes of age' available at https://www.mckinsey.com/~/media/McKinsey/Business%20Functions/McKinsey%20Analytics/Our%20Insights/Analytics%20comes%20of%20age/Analytics-comes-of-age.ashx (accessed 6th August, 2019).
17. Parish, R. (2019) 'Forrester's top customer experience research findings of 2018', available at: https://go.forrester.com/blogs/forresters-top-customer-experience-research-findings-of-2018/ (accessed 6th August, 2019).
18. Brown, D. (2018) 'Americans are more concerned with data privacy than job creation, study shows', *USA Today*, available at https://www.usatoday.com/story/money/2018/11/09/americans-more-concerned-data-privacy-than-healthcare-study-says/1904796002/ (accessed 6th August, 2019).
19. Snider, M. (2018) 'Your data was probably stolen in cyberattack in 2018—and you should care', available at https://www.usatoday.com/story/money/2018/12/28/data-breaches-2018-billions-hit-growing-number-cyberattacks/2413411002/ (accessed 26th August, 2019).