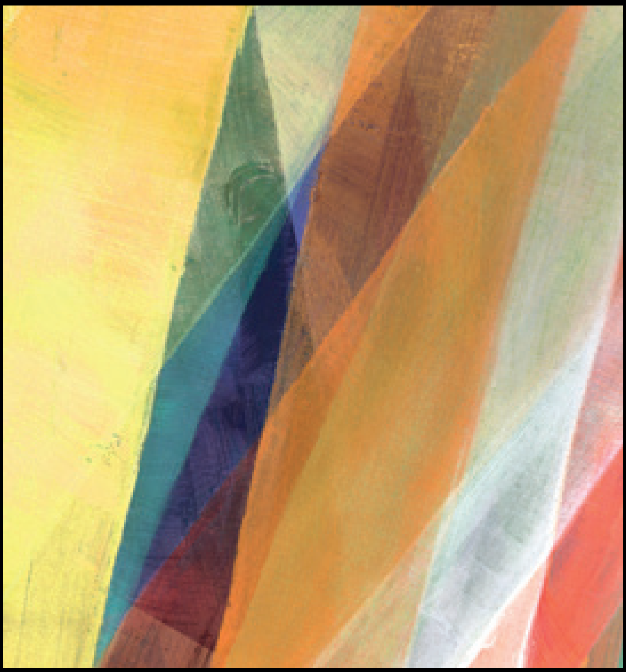
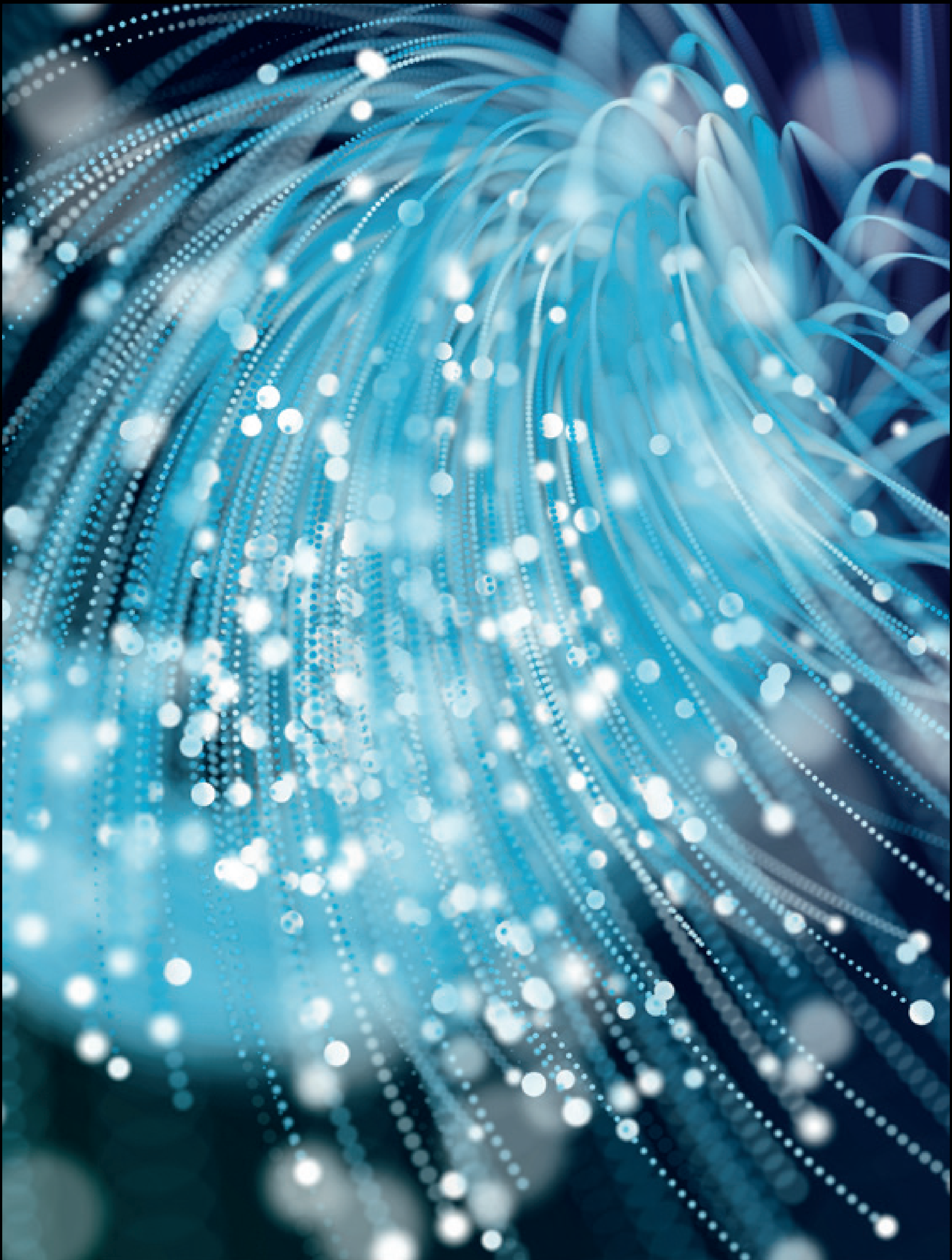
CAPCO

CAPCO INTELLIGENCE Nº 3

CAPCO

THIS ISSUE





A UK SURVEY OF CONSUMER ATTITUDES TO BNPL

AUTHORS:
Rachel Baugh, UK
Howard Rees, UK
Harriet Webster, UK

METHODOLOGY

During September and October 2020, Capco conducted a survey on the rise of Buy Now, Pay Later (BNPL) personal finance offerings. We set out to understand BNPL usage and where it fits in the wider consumer credit industry, as well as key trends for consumer spending habits and differing levels of financial education. The report represents a broad range of respondents, across six individual age demographics (18-24, 25-34, 35-44, 45-54, 55-64, 65+).

The survey was conducted in conjunction with **Brandwatch Qriously**[1], a market research and polling company that offers an online service to measure location-based public sentiments in real-time. We collected responses from 2,016 individuals; all were UK-based, with the majority located in and around England's major cities, including London, Manchester, and Birmingham.

Out of the total sample size, 996 of respondents were male and 1020 were female. Individuals were distributed fairly evenly across our six age categories, with the 65+ demographic accounting for the highest proportion of respondents. However, the sample size varied between each question, depending on how the respondent answered. This feature, known as 'skip logic', changes the question a respondent sees next based on how they answer a question.

> *"BNPL providers have risen in popularity over the past few years, growing by 39 percent annually in the UK alone."*

INTRODUCTION

Buy Now Pay Later (BNPL) is a point-of-sale personal finance proposition, which like its title suggests, allows consumers to take a product and delay or stagger the payment. This flexible credit option has grown in prominence and popularity in recent years, namely with the emergence of Klarna, a Swedish digital bank and leading BNPL provider which came to the UK in 2014.[2] Over the past year, more than ten million people in the UK have purchased products or services through a BNPL scheme.[3]

Globally, BNPL is a fast-moving market, and today's providers are predominantly non-traditional lenders, such as fintechs and challenger banks. In October 2020, PayPal began offering three-part instalments in the UK (known as PayPal Credit 'Pay in 3')[4], and Danish challenger Lunar's CEO shared his plans to enter the Nordic BNPL market.[5] Over in Australia meanwhile, there was news that the bank Westpac had signed BNPL firm Afterpay as the first user of its banking-as-a-service (BaaS) platform to offer "customer-centric alternatives to traditional banking products" in 2021.[6]

So, what's so special about BNPL? The transparency of repayment mechanisms and slick customer journey present a new and appealing route to credit that attracts a broad customer base. A study conducted by Klarna and Researchscape[7] revealed that 47 percent of people surveyed would like to be presented with an instant financing option whilst shopping online.

Unlike conventional credit checks, BNPL's online credit assessments are carried out in real-time and often have no impact on an individual's credit rating. BNPL products offer consumers instant financing results in near-immediate purchase approval that has the additional upside of helping merchants to increase conversions and drive more sales. Then when payments are due, BNPL sends alerts (by email or app) and offers automated repayment options to minimize the risk of missed payments and hence potential debt.

There have, however, been concerns about the transparency of BNPL payment terms. In June 2019, the Financial Conduct Authority (FCA) published its feedback and final rules[8] on BNPL credit, to provide clearer information to consumers about BNPL offers; forbid providers from backdating interest on amounts of money that have been repaid by the consumer during the BNPL offer period; and make sure providers are proactively reminding customers when their BNPL offer period is about to end. In July 2020, the FCA issued temporary guidance for BNPL providers on customers financially impacted by COVID-19[9], and have laterally proposed extended leniency measures due to the second UK lockdown[10]. Unsecured credit providers have also been told to expect further updates from the FCA in 2021[11].

This enhanced regulatory focus, coupled with growing BNPL usage, demonstrates that BNPL is here to stay. As new market entrants continue to disrupt this space, we have taken this opportunity to delve deeper into what consumers think, where BNPL fits within the wider consumer credit industry, and how banks – as trusted providers – can themselves take advantage of this new lending channel.

EXECUTIVE SUMMARY

Since 2014, when Klarna first launched in the UK, a wave of similar BNPL start-ups have succeeded in accessing funding and avoiding strict regulation to accelerate their growth. Indeed, Worldpay's 2020 payments report[12] revealed that BNPL providers in the UK are on course to double their market share of online purchases by 2023. But as regulators begin to impose stricter rules within this sector, and as the economic fallout of COVID-19 continues, what does this mean for the future of BNPL – and what opportunity does it present for banks?

The ethics of BNPL are very much the focus of public debate and scrutiny: a 'new death trap for millennials' and 'selling debt as a quick fix during an economic crisis'[13],[14] are two of the less flattering judgements. The marketing and messaging around BNPL is often friendly and conversational in tone, with an emphasis on convenience, personalization, and ease. But the attraction for merchants is clear: leading BNPL player Klarna claims to increase average order value by 68 percent[15]. BNPL providers also seek to leverage the power of influencer marketing, which raises ethical questions, particularly given the youthful profile of some of the customer segments targeted by providers. However, that is not to suggest that opinions around BNPL are necessarily negative.

OUR KEY FINDINGS

BNPL COULD RISK PUTTING PEOPLE INTO DEBT.

Almost half of young respondents (18 – 34) have missed a BNPL payment.

FINANCIAL EDUCATION IS LACKING.

There is a popular misconception about BNPL – 44 percent are unsure whether BNPL means 'taking on debt' or 'deferring a payment'. Among young people (18 – 34 years) this rises to a total of 57 percent.

CONSUMERS WOULD WELCOME BNPL REGULATION.

Over half of consumers surveyed want BNPL products to be regulated (54 percent); and 52 percent want providers to consider their credit history before financing is approved.

THE CREDIT CARD CONTINUES TO BE THE MOST POPULAR FORM OF CREDIT…

74 percent of our respondents use a credit card.

…BUT BNPL IS GAINING GROUND.

Almost half of BNPL users say BNPL is their preferred form of credit (46 percent) and would like BNPL integrated into their current account or credit card (45 percent).

THE PANDEMIC HAS PROMPTED INCREASED USE AMONG SOME CONSUMERS.

32 percent of respondents say it has increased their spending during COVID-19.

OUR KEY FINDINGS CONTINUED

MARKET LEADING BRANDS ARE ALREADY ESTABLISHED. Klarna is the most popular BNPL product with young people; PayPal credit is the most well-known provider across all generations surveyed.

We believe banks should be making a defensive 'play' in this space to maintain their existing market share. A number of paths present themselves:

1. Investing in instalment-based products within their existing suite of offerings

2. Creating their own standalone BNPL products

3. Partnering with a BNPL provider to provide either of the above services

4. Further refining their credit card offerings to enhance their appeal to new and existing customers.

ABOUT OUR RESPONDENTS

A 2020 study[16] conducted by pymnts.com revealed that 67 percent of millennials surveyed used BNPL products while shopping. In our study, we wanted to consider the impact of BNPL on a much wider demographic, spanning respondents between the ages of 18 and 65+. We were keen to gauge whether the most popular consumer credit offering – the revolving credit card – was still as popular with consumers, or whether it is now being challenged by BNPL solutions.

Although it might be assumed that BNPL attracts mostly millennial consumers, we found that within our sample of 2,016 individuals, most of those who have used BNPL in the past were in the 65+ age bracket (23 percent), followed by the 25-34s (18 percent) and then the 45-54s (17 percent).

The survey drew a near even split between males and females – 996 for males and 1,020 for females. This helped to give a more accurate representation when looking at the consumer trends of both demographics. Although there wasn't huge variation between genders across our age groups, we found that the older demographics skewed slightly towards a higher percentage of female respondents.

We asked respondents to share their annual individual income between the following salary brackets: up to £15,000; £15,000 – £24,999; £25,000 – £34,999; £35,000 - £44,999; £45,000 - £59,999; and £60,000+. Almost half of respondents (49 percent) chose not to disclose this information; across the remaining 52 percent of respondents, the majority (21 percent) of respondents selected between £15,000 and £35,000 for their incomes.

WHAT DOES BNPL MEAN FOR BANKS?

We know that UK lenders are evaluating opportunities to develop their own instalments propositions, ranging from in-purchase on debit and credit cards, to post-purchase and to standalone capability.

Our survey revealed that almost half of the respondents we surveyed do not use any form of credit, and almost 50 percent of these respondents did not want BNPL linked with their credit card or in their current account.

However, among respondents who had used BNPL previously, 34 percent said they would welcome BNPL being an integrated feature with their current account or credit card (and 26 percent said not sure).

Interestingly, for those who have used the two most well-known providers of this survey group (Paypal Credit and Klarna) this rises to almost a 50 percent 'yes' response (44 percent and 49 percent respectively), which demonstrates the impact BNPL has had on their payment choices.

The survey has also revealed that BNPL could be eroding credit card usage, with almost half of respondents who have used BNPL previously stating that they would rather use BNPL over another form of credit (46 percent).

To sustain the profitability of their credit card businesses, banks and other credit providers should consider offering customers the ability to integrate a BNPL payments proposition within their current account or credit card, as a flexible feature, to provide tailored lending propositions to specific customer segments; and to build a standalone feature outside of their traditional card offerings.

Our survey highlighted a number of different consumer behaviours. Despite the rapid rise of BNPL, our data showed that almost half of respondents (45 percent) only use BNPL either a few times a year or less than once a year. However, the rate of BNPL usage is based on how often consumers can use these services, and we know that not everything can be paid for using BNPL. As BNPL providers expand into more consumer 'verticals', and consumers begin using BNPL across a wider range of purchases, the rate of usage will presumably increase.

BNPL has gained traction across retail industries such as fashion, health & beauty, toys, and electricals[17] but adoption has been slower for larger purchases. Having said that, Klarna seems to be testing the glass ceiling to the available market for BNPL, with Klarna Financing, which is available on products such as bikes (Peloton, Brompton, Raleigh and Halfords), electronics (Samsung) and furniture (Loaf).[18] In order to increase the rate of usage of BNPL, providers will need to look to build a bigger presence in physical stores and enter new industries.

For industries that already have a financing industry behind them – the automotive sector being a prime example – BNPL could struggle to make a real impact. Car financing, for example, is already tied to customer experience. However, we believe there is a compelling case for banks to compete with BNPL providers by expanding into other industries that BNPL may not currently operate in, as their mature credit risk and underwriting capabilities – paired with their access to vast amounts of consumer data – will enable them to better assess risk and offer appropriate lending to their customers.

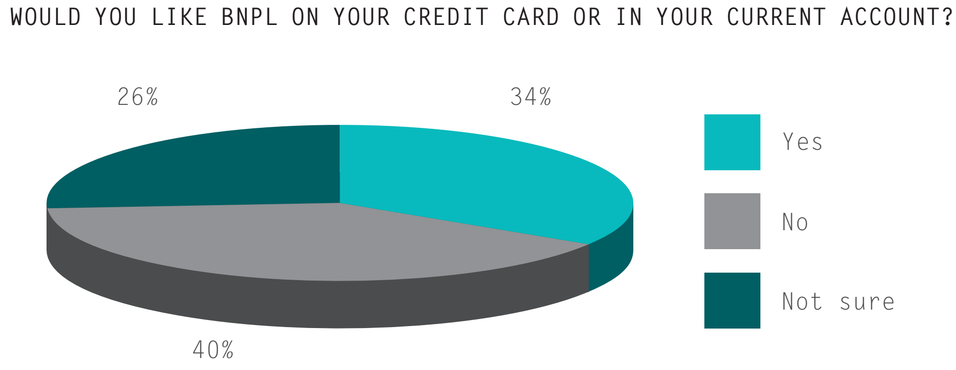


Figure 1. Results filtered by respondents who have used BNPL products.

CURRENT PROVIDERS

BNPL providers have risen in popularity over the past few years, growing by 39 percent annually[19] in the UK alone. Swedish bank, Klarna, was ranked as one of the most highly valued fintechs in Europe with a valuation of $5.5 billion[20] – yet just 10 percent of survey respondents said they had used Klarna. Our survey also revealed that after credit card and point of sale (PoS) finance, PayPal Credit was the most used BNPL provider (19 percent), followed by Klarna (11 percent).

When we looked at the data for some of the other smaller providers, usage dropped further. Only 6 percent of respondents had used ClearPay, 4 percent had used V12 and 3 percent had used OpenPay or LayBuy.

Our research also highlighted which of the BNPL providers customers have missed payments with. Having identified the top three; ClearPay, Klarna and PayPal Credit, we were keen to see how user experience impacts the user journey and how that relates to repayment behaviours.

Of the three, ClearPay users led the pack in terms of non-payments, with 41 percent saying they had missed a payment. They were followed by PayPal Credit users (29 percent of users) and then Klarna users (27 percent of users).

One interpretation of this data is that repayment may not be as evident as necessary. For some of these providers, (such as Klarna) when you defer a payment for 30 days, the consumer is given the option to turn off auto-pay[21]. Repayment then becomes the consumers responsibility; it is not an automatic payment taken from the consumers bank account. By placing the onus on the consumer, it is likely that they may forget to make a repayment, which could lead to financial implications.

HOW MANY OF THESE CREDIT AND / OR BNPL PROVIDERS HAVE YOU USED?

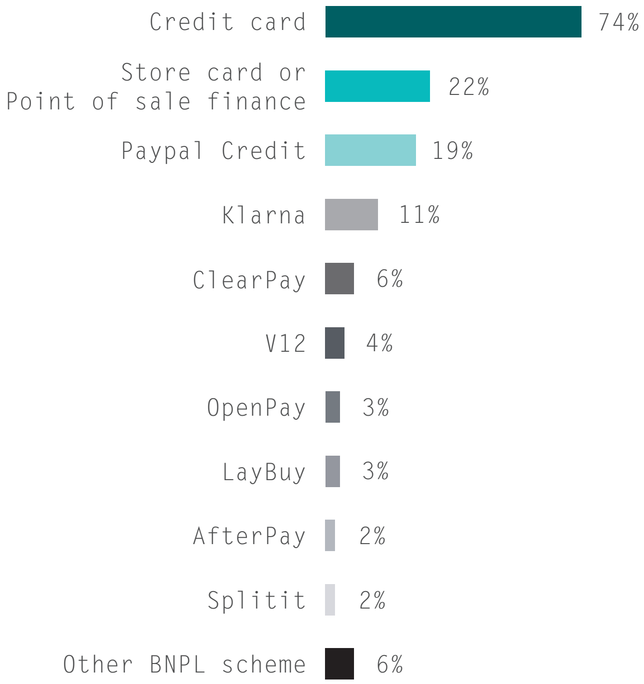


Figure 2. Survey respondents could select multiple credit types

HAVE YOU EVER MISSED A BNPL PAYMENT?

Figure 3. Results for respondents who had previously used ClearPay

HAVE YOU EVER MISSED A BNPL PAYMENT?

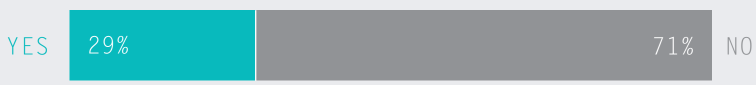


Figure 4. Results for respondents who had previously used PayPal Credit

HAVE YOU EVER MISSED A BNPL PAYMENT?

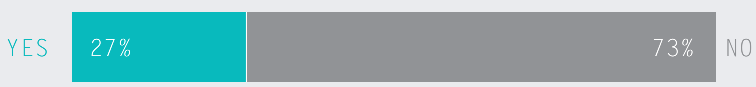


Figure 5. Results for respondents who had previously used Klarna

ABOUT OUR RESPONDENTS

We also looked at how customers choose to pay, whether via instalments or one lump-sum payment. The majority (71 percent) said they prefer to split the cost into instalments, which all the above providers offer, whether over three, four, or six months.

If this consumer preference towards instalments continues, it could pose a threat to incumbents and credit card profitability by attacking their interest income and enabling less affluent demographics to split costs and access credit.

IS BNPL VIEWED AS 'TAKING ON DEBT'?

We asked respondents whether BNPL has made them spend more, to which 56 percent said 'No'. Yet the remaining proportion, 44 percent, said 'Yes', which is still a fairly substantial figure. Is this because consumers don't view BNPL as taking on debt? We asked them this very question – do you think BNPL is taking on debt, or just deferring a payment? Our data revealed that 44 percent said they weren't sure, which could suggest a lack of financial education and could be a cause for concern given that a third of our respondents have used BNPL before. When we broke it down further into the 18-34 group, 57 percent of respondents said, 'not sure'.

A report by the financial advice site Money.co.uk, "Shop now, stress later[22]", suggests that 18 to 24-year-olds on BNPL schemes such as Klarna, Clearpay, Zilch and Laybuy owe about £225 each. Despite often being labelled as a generation of 'savvy shoppers', Money.co.uk suggests that the temptation of using BNPL could be leading consumers into a 'dangerous cycle of unmanageable debt[23]'.

When we looked at the data for our youngest demographic, the 18-34-year olds, almost two-thirds of respondents said that BNPL had made them spend more (62 percent). Similarly, 50 percent of this same cohort we surveyed also admitted to missing a payment.

Is this a result of enticing brand marketing from popular retailers or are the repercussions for non-payment not taken as seriously as those associated with more traditional forms of credit? For PayPal Credit, Laybuy and Clearpay, there are financial penalties for late payments and customers can be referred to credit agencies[24] (although Clearpay have stated this has not ever happened in their four years of operations[25]). Klarna[26] stated that there is no impact on credit score could potentially encourage bad spending habits, such as revolving debt and an unhealthy attitude towards it.

On the other hand, growth in BNPL usage amongst younger consumers could be a positive. The ability to manage small amounts of debt, without the stress or worry of negatively impacting their credit score, could in theory, assist in improving their financial literacy and money management abilities. However, this would require an existing understanding of debt and good money management!

WHEN USING BNPL, HOW DO YOU TYPICALLY OPT TO PAY?

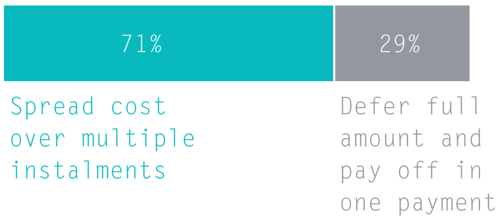


Figure 6. Question asked to all respondents who had previously used a BNPL provider

HAVE BNPL SERVICES MADE YOU SPEND MORE?

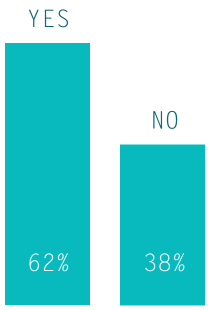


Figure 7. Our Qriously survey responses from 18-34-year-olds

HAVE YOU EVER MISSED A BNPL PAYMENT?

Figure 8. Our Qriously survey responses from 18-34-year-olds

REGULATION

BNPL is transforming the way consumers pay. It is rising in both popularity and convenience, yet because of its newness has not been as regulated as more traditional credit products, such as the credit card. To date, the majority of BNPL providers do not charge customers interest, and therefore currently fall beyond the remit of regulation by the Financial Conduct Authority (FCA). But what does this mean for consumers, and how do they feel about using these offerings?

54 percent of our respondents said they wanted BNPL to be regulated. An even higher majority of those who use BNPL or other forms of credit support BNPL regulation too (71 percent).

However, we thought it was interesting that out of all respondents for this question, 33 percent were 'not sure' whether BNPL should be regulated. This implies that there is a potential lack of financial education around the risks or understanding of the role of regulatory authorities.

The survey results also revealed that a third of respondents who had used BNPL or credit cards had missed a payment, which may be because of a lack of transparency around penalties. This could have an adverse impact on consumer's credit scores and their long-term ability to borrow, which is one of the key reasons why the FCA are currently reviewing this new lending proposition.

As BNPL services continue to grow, providers can expect to face greater regulatory scrutiny in terms of transparency and customer treatment, which may create issues for both the providers and their customers. We're seeing buy now, pay later companies like Klarna face a crackdown by the Financial Conduct Authority, as part of a sweeping inquiry[27] into lending practices in the unsecured credit market. And in April 2020, the FCA announced that this review[28] will be an important building block for the FCA's Consumer Credit business priority.

DO YOU THINK BNPL PROVIDERS SHOULD BE REGULATED?

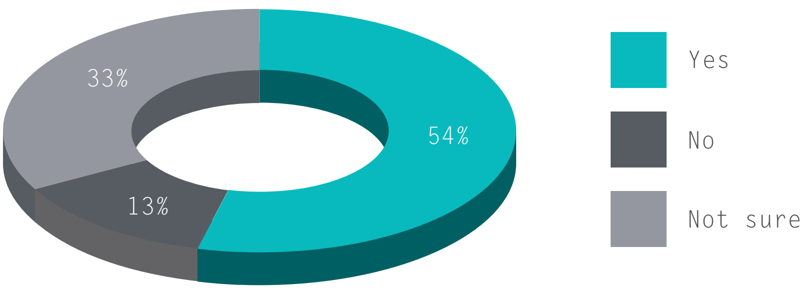


Figure 9. Question asked to all respondents

THE IMPACT OF COVID-19 ON BNPL

It is no secret that the COVID-19 pandemic has had, and will continue to have, a highly detrimental impact on individuals, businesses and the economy in general. The combination of economic downturn, paired with the restrictions on going out, has likely spiked ecommerce volumes, resulting in an increase in BNPL usage. In fact, research conducted by retail insights firm Edge by Ascential predicts[29] that the COVID-19 pandemic is expected to add £5.3 billion to UK ecommerce sales in 2020, bringing sales to a total of £78.9 billion.

However, this comes with its own risks, as consumers may not realize what they are spending. In 2020 in the UK, the unemployment rate rose to 4.5 percent between June and August, ONS[30], an estimated 1.5 million people were unemployed between June and August, while redundancies stood at 227,000.

We were interested to find out how BNPL usage may have changed during COVID-19, given the current economic uncertainty.

As Figure 10 shows, it appears that BNPL usage has not increased during COVID-19 amongst our consumer sample group, with almost 60 percent of respondents responding 'No'. On the other hand, almost one-third of people surveyed that said their usage increased during COVID-19, which aligns with media reports of increased BNPL spending during the COVID-19 period[31].

BNPL products offer consumers the ability to make a purchase and pay it off via a pre-agreed number of interest-free instalments, making such transactions both affordable and seamless. However, when onboarding a new customer, there is also a need to consider the potential future state of an individual's finances (especially given the current UK recession and warnings of an imminent 'Second Wave' of COVID-19[32]). The FCA have consequently launched a review into the unsecured lending market, and namely BNPL for this reason.[33] Klarna has said it had tightened its rules on lending as a result of COVID-19.[34] The question is, will other providers be following suit?

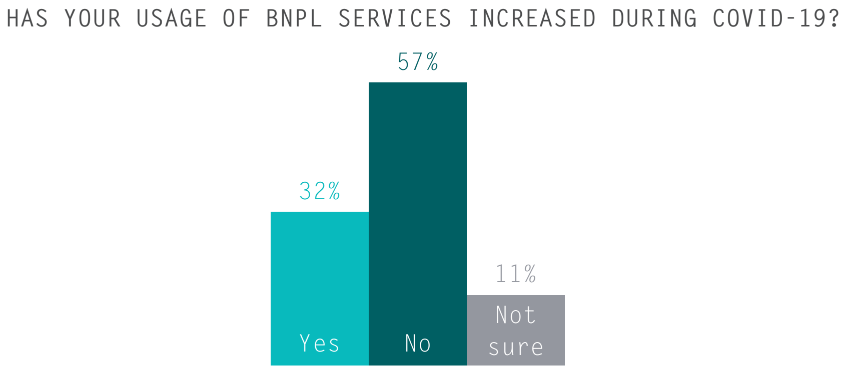


Figure 10. Answers from respondents who have used BNPL previously

CONCLUSION

We are seeing more banks enter the BNPL and instalments space, which suggests BNPL is viewed not simply as a fad but recognized as a segment that is growing faster than any other online payment method[35]. Such is the depth of that BNPL footprint that reportedly, almost one in five UK consumers say that they would not shop with a retailer who didn't offer a BNPL option[36] – this should act as a wakeup call for not only retailers but as a potentially lucrative opportunity within the larger credit market.

The combination of BNPL's frictionless customer experience, point-of-sale business model and competitive, interest-free lending terms could be putting traditional credit forms under threat. Banks and credit card companies now need to think more strategically about their market offerings. While instalments and BNPL are a relatively new lending channel, they would not require banks to completely remodel their current business models to make a defensive play in this space.

As displayed in Figure 11 below, our survey has highlighted that credit card users who have also used BNPL could be moving away from high-interest credit because BNPL is an easy-to-use and flexible way to pay. Given recent news that the cost of credit card borrowing will be increasing as the winter holidays approach[37], coupled with a record-number of credit card users paying off the debt during UK lockdown[38], credit card usage is expected to continue to drop[39].

Credit cards still have a place in today's financial services landscape however, and providers have an opportunity to further cater to specific customer segments and personas that cannot be accommodated by BNPL offerings, such as the facility to offer points and cashback incentives to reward regular use. After all, our survey found that BNPL use is largely sporadic and there will be customers who still depend on their credit card for day-to-day or more frequent expenditure (such as bills), but BNPL could be eating away at card margins[40].

For this reason, along with the industry's increased regulatory scrutiny (in the aftermath of the Payment Protection Insurance controversy and consumer debts spiraling) and consumer appetite for such, banks and other lenders that already conduct credit checks, and have a longstanding relationship with the regulator are in a good spot to provide trusted BNPL solutions and can leverage this as a competitive strength.

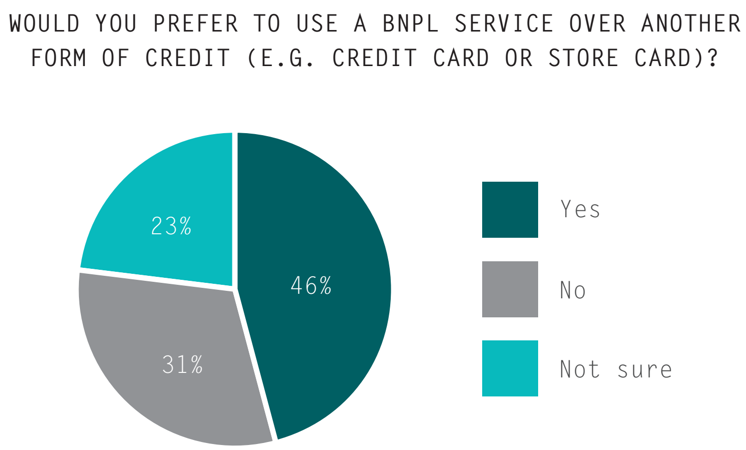


Figure 11. Responses by BNPL users, excluding credit card users

CONCLUSION CONTINUED

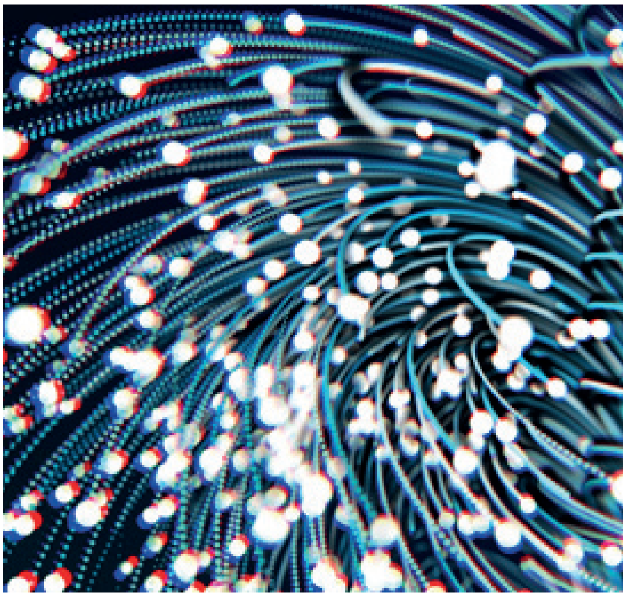
While BNPLs may be operating in a grey area today, this won't be for long. Now's the time for banks and other trusted financial services firms to manage the shift towards a more diverse lending landscape, by:

1. Looking at investing in instalments solutions

2. Creating standalone BNPL products

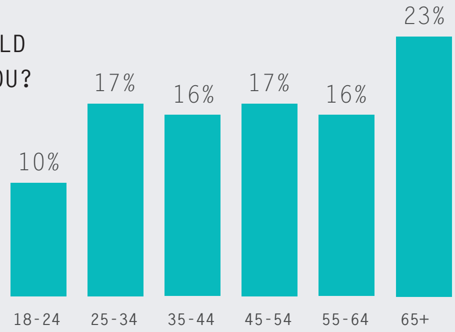
3. Partnering with a BNPL provider to provide either of the above services

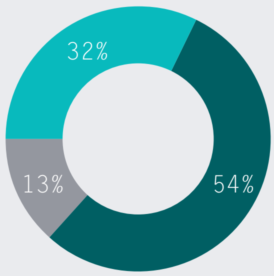
4. Further refining credit card offerings to appeal to new and existing customers.



APPENDIX

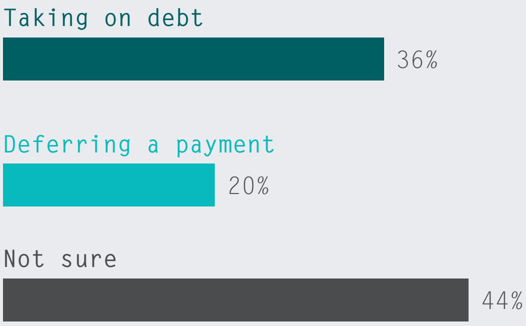
HOW OLD ARE YOU?

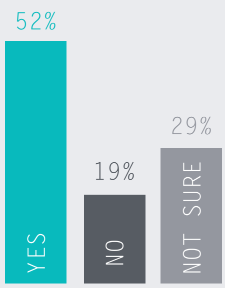




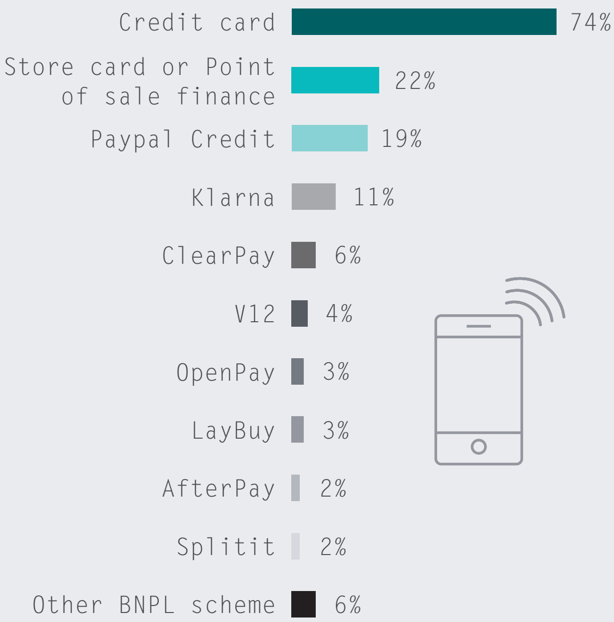
HAVE YOU USED CREDIT (I.E. CREDIT CARD) OR ANY 'BUY NOW PAY LATER' PROVIDERS BEFORE?

DO YOU THINK OF 'BUY NOW PAY LATER' (BNPL) AS TAKING ON DEBT OR DEFERRING A PAYMENT?



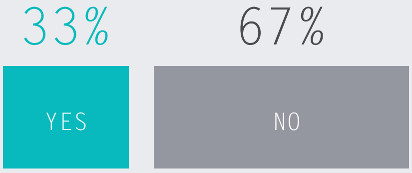


DO YOU THINK THAT A BNPL PROVIDER SHOULD CONSIDER YOUR CREDIT HISTORY BEFORE LETTING YOU USE THEIR SERVICE?



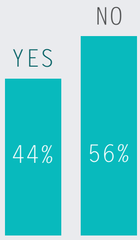
HOW MANY OF THESE CREDIT AND / OR BNPL PROVIDERS HAVE YOU USED?

APPENDIX CONTINUED

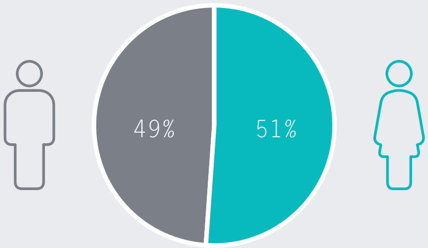


HAVE YOU EVER MISSED A BNPL PAYMENT?

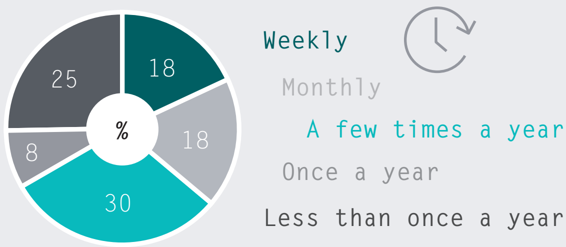
HAVE BNPL SERVICES MADE YOU SPEND MORE?



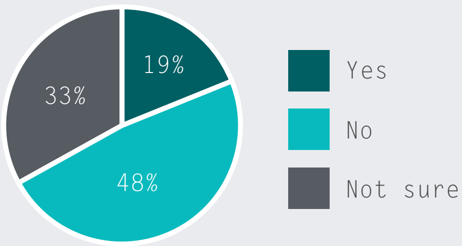
ARE YOU MALE OR FEMALE?

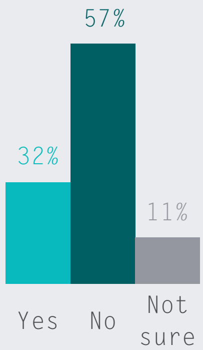


HOW OFTEN DO YOU USE THESE PROVIDERS?



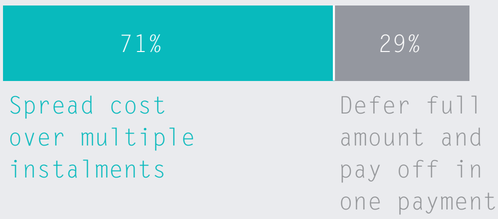
WOULD YOU LIKE BNPL ON YOUR CREDIT CARD OR IN YOUR CURRENT ACCOUNT?





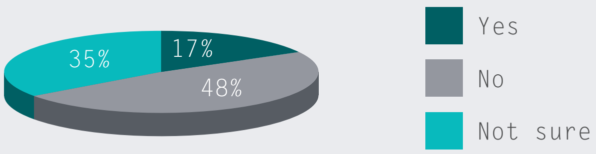
HAS YOUR USAGE OF BNPL SERVICES INCREASED DURING COVID-19?

WHEN USING BNPL, HOW DO YOU TYPICALLY OPT TO PAY?

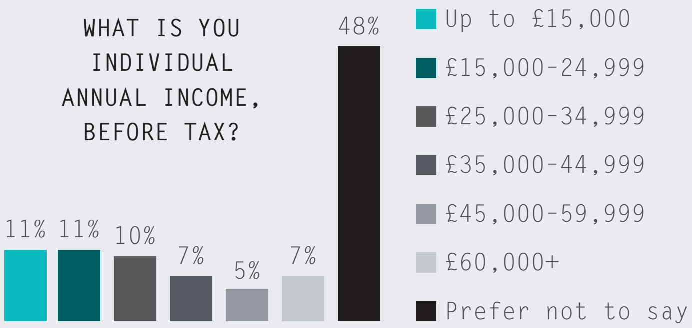


APPENDIX CONTINUED

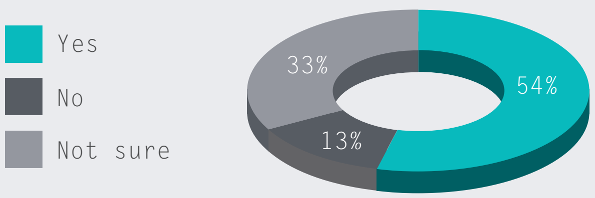
WOULD YOU PREFER TO USE A BNPL SERVICE OVER ANOTHER FORM OF CREDIT (E.G. CREDIT CARD OR STORE CARD)?



WHAT IS YOU INDIVIDUAL ANNUAL INCOME, BEFORE TAX?



DO YOU THINK BNPL PROVIDERS SHOULD BE REGULATED?



REFERENCES

1. https://www.brandwatch.com/products/qriously/
2. https://www.nytimes.com/2014/08/25/technology/klarna-an-online-payment-system-popular-in-europe-eyes-global-expansion.html
3. https://www.which.co.uk/news/2020/01/can-shopping-with-klarna-clearpay-or-laybuy-hurt-your-credit-score/
4. https://www.pymnts.com/news/payment-methods/2020/paypal-expands-bnpl-pay-in-3-option-to-uk/
5. https://techcrunch.com/2020/10/23/nordic-challenger-bank-lunar-raises-e40m-series-c/amp/?__twitter_impression=true&s=08&guccounter=1
6. https://www.fintechfutures.com/2020/10/afterpay-signs-up-to-westpac-banking-as-a-service-platform/
7. https://www.klarna.com/knowledge/articles/instant-financing-heres-what-you-didnt-know/
8. https://www.fca.org.uk/news/press-releases/fca-publishes-final-rules-buy-now-pay-later-products
9. https://www.fca.org.uk/publications/finalised-guidance/rent-own-buy-now-pay-later-and-pawnbroking-agreements-and-coronavirus-updated-temporary-guidance
10. https://www.pymnts.com/loans/2020/united-kingdom-financial-conduct-authority-gives-six-more-months-loan-holidays/
11. https://www.fca.org.uk/publication/call-for-input/woolard-review-unsecured-credit.pdf
12. https://worldpaymentsreport.com/resources/world-payments-report-2020/
13. https://www.ft.com/content/8c751ac6-bb63-11e8-94b2-17176fbf93f5
14. https://inews.co.uk/opinion/buy-now-pay-later-schemes-klarna-debt-economic-crisis-465356
15. https://www.klarna.com/uk/business/campaign-instalments/
16. https://securecdn.pymnts.com/wp-content/uploads/2020/01/PYMNTS-Buy-Now-Pay-Later-January-2020-Tracker.pdf
17. https://www.thisismoney.co.uk/money/cardsloans/article-7966159/Could-buy-pay-later-Klarna-kill-credit-card.html
18. https://www.klarna.com/uk/business/products/financing/
19. https://thefintechtimes.com/use-of-buy-now-pay-later-products-in-the-uk-set-to-more-than-double-by-2023-finds-new-worldpay-report/
20. https://www.klarna.com/international/press/new-klarna-data-reveal-that-79-of-consumers-would-rather-be-healthy-than-wealthy-this-holiday-season/
21. https://www.klarna.com/us/customer-service/how-can-i-schedule-automatic-payments-autopay-or-turn-it-off/
22. https://www.money.co.uk/guides/generation-debt-trap
23. https://www.money.co.uk/guides/generation-debt-trap
24. The Era of Buy Now, Pay Later, Capco whitepaper, November 2020.
25. https://www.which.co.uk/news/2020/01/can-shopping-with-klarna-clearpay-or-laybuy-hurt-your-credit-score/
26. https://www.theguardian.com/money/2020/oct/03/klarna-debt-buy-now-pay-later-fees-interest
27. https://www.thetimes.co.uk/article/klarna-in-spotlight-as-fca-launches-crackdown-on-unsecured-credit-0dslvllqn
28. https://www.fca.org.uk/news/press-releases/christopher-woolard-chair-review-unsecured-credit-market-regulation

REFERENCES CONTINUED

[29] https://www.prnewswire.com/news-releases/covid-19-to-add-5-3bn-to-uk-ecommerce-in-2020--301080427.html

[30] https://www.ons.gov.uk/economy/grossdomesticproductgdp/articles/coronavirusandtheimpactonoutputintheukeconomy/june2020

[31] https://www.yourmoney.com/credit-cards-loans/young-adults-turn-to-buy-now-pay-later-schemes-during-lockdown/

[32] https://www.theguardian.com/world/2020/oct/21/warning-of-tens-of-thousands-of-deaths-in-england-from-covid-19-second-wave

[33] https://www.globalbankingandfinance.com/paypal-launches-pay-in-3-buy-now-pay-later-loans-to-uk-in-time-for-black-friday-and-christmas/

[34] https://www.bbc.co.uk/news/technology-53465978

[35] https://www.pymnts.com/today-in-data/2020/rising-popularity-of-buy-now-pay-later/

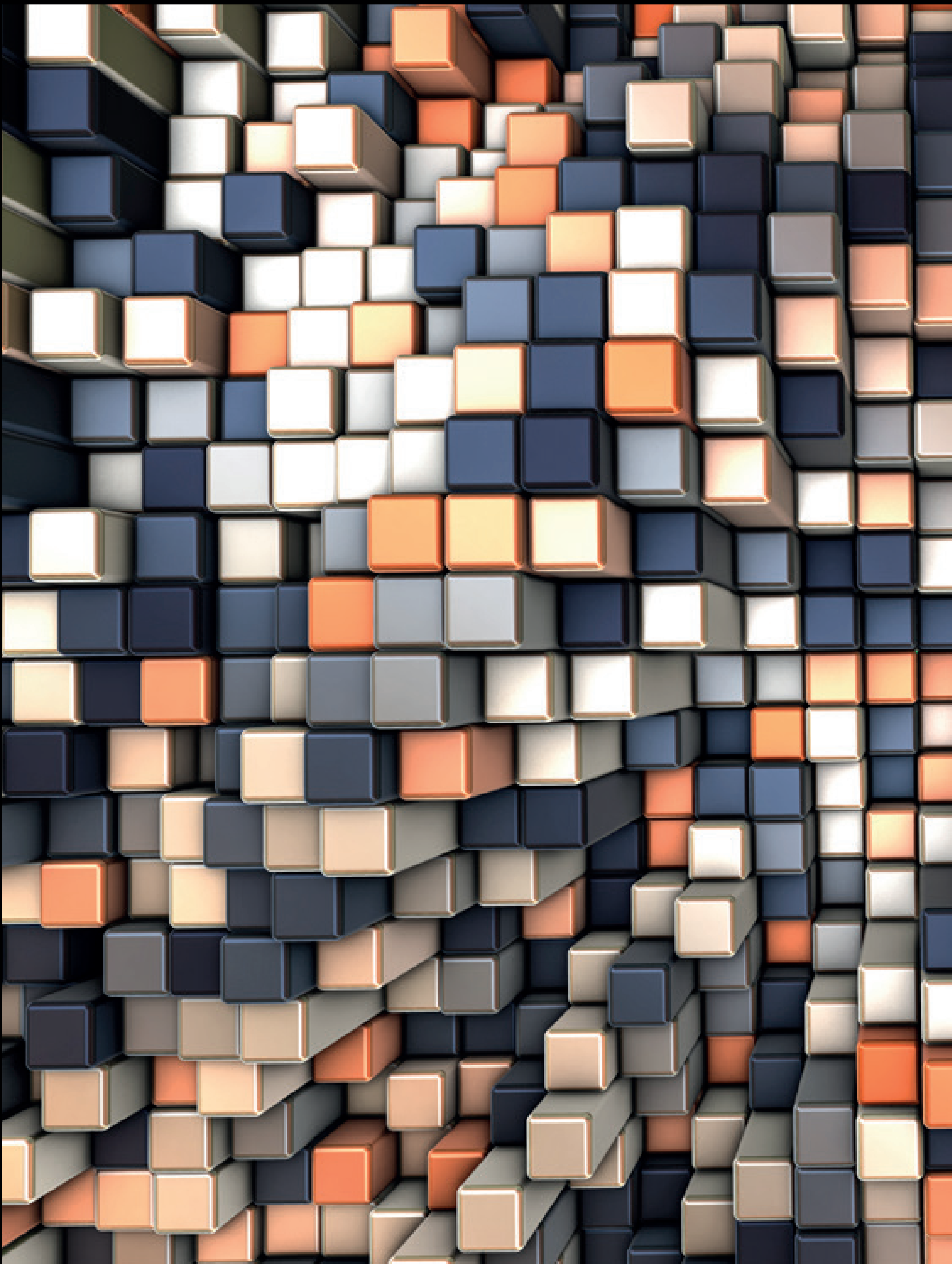
[36] https://www.thisismoney.co.uk/money/cardsloans/article-7966159/Could-buy-pay-later-Klarna-kill-credit-card.html

[37] https://www.theguardian.com/money/2020/oct/15/uk-banks-plan-to-hike-cost-of-credit-card-borrowing

[38] https://www.ukfinance.org.uk/covid-19/consumers-paid-down-credit-card-bills-during-lockdown

[39] https://www.bbc.co.uk/news/business-53416676

[40] https://www.afr.com/companies/financial-services/1-7b-of-bank-card-revenue-under-pressure-20200116-p53s02



DATA ETHICS IN FINANCIAL SERVICES

AUTHORS:
Simon Campbell, Canada
Anna Chen, Canada
Sonia Chau, Canada
Lyn Pham, Canada
Lavesh Bansal, Canada
Eddie Kim, Canada
Joanna Lewis, Canada

Technology has been developing at an increasingly rapid pace across the world, and along with it, data generation, storage, and integration into everyday business operations. As organizations continue to invest more in their data capabilities and AI regulations try to keep pace globally, financial institutions (FIs) need to ensure they have a framework in place to manage data ethically across its lifecycle.

FIs have a fiduciary duty to their clients, and are expected by society and governing bodies to act in the best interest of their clients. However, as FIs operate across economic and cultural boundaries, data regulations can be expected to differ, and consumers across regions have begun raising concerns around how companies are collecting, using, and sharing their data. Consumers' increase in cautiousness can lead them to lobby for more stringent government policies on how companies can use client data and how transparent they must be when doing so.

Having large credit card and credit bureau companies headlining on their lack of proper storage and security of sensitive client data exasperates the desire for more stringent government regulations. Consumers now have heightened awareness of their rights and are increasingly wary of providing their personal information to firms they do not trust entirely to handle their data. There are specific laws in various geographic regions that outline fundamental privacy rights such as the Personal Information Protection and Electronic Documents Act (PIPEDA) in Canada, the Privacy Act in the United States, and the General Data Protection Regulation (GDPR) in Europe. Although business leaders are likely inclined to want to use the highest volume of data along with the most advanced data analytics techniques to help them to make improved business decisions, they need to be cognisant not to misuse the data entrusted to them.

Consumers are becoming increasingly wary of the potential pitfalls of big data companies (Nichols, 2018), and as a result are becoming more demanding that their data be managed ethically and with transparency. This has led to an increasingly common trend; consumers threatening to discontinue doing business with organizations that do not meet their data ethics expectations. This could lead to significant and unrecoverable losses if FIs are not careful with how they are treating their clients' data with respect to both customer desires and regulations. Therefore, FIs must be aware of what their customers expect when it comes to data privacy, and must follow regulations to avoid potential lawsuits and damage to their brand.

However, the pace of technological advancement means that laws and regulations can quickly become obsolete, leaving grey areas for day-to-day operational decisions. FIs are now capable of making better use of customer data to help them increase customer satisfaction and profitability, and how they collect and use customer data has changed drastically. Therefore, FIs must ensure they are not only up to date with the policies within the regions they are operating, but have a robust ethical framework in place that spans across the organization to mitigate the risk of running into ethical issues when and where the laws are out of date because they have not accounted for the latest technologies or associated capabilities.

Another consideration for FIs is coordinating the sharing of data with third-party vendors in 'open-banking' ecosystems. FIs must ensure that they are moving this data securely and that the organizations they share data with will follow equally stringent privacy policies with their clients' data.

This brings us to question how FIs can ensure that they are not only following data laws, but also instilling trust in their customers and the public at large, that they are guarding and using their personal information ethically.

PILLARS FOR ETHICAL DATA MANAGEMENT

To address this we have established five pillars that FIs should leverage at the top of the organization and across geographies and lines of business to ethically manage data. As such, these pillars for ethical data management are agnostic to the domain or business units to facilitate organization-wide adoption. The pillars are: transparency, regulations, fairness and reliability, security and privacy, and accountability.

TRANSPARENCY

Being transparent with data means ensuring that how data is being collected, stored, transformed and used is thoroughly documented. This documentation (in a digestible and accurate format) must be accessible to both regulatory bodies and consumers whose data the FI uses to derive insights, make predictions, or decisions. Examples of poor data transparency have proven to have damaging consequences to the firms involved. The Facebook/Cambridge Analytica incident in 2018 is a prime example where personal user data of the social media platform was shared with the third-party (Cambridge Analytica), without user knowledge. This resulted in an overall loss of trust from Facebook users and a drop in stock price, while serving as a flag to global regulators that regulations around transparency required modernization (Kozlowska, 2018).

Because of this, we now know that transparency requires going beyond the raw data itself, and must include the processing and transformation of data, as well as the intent behind any analytics or AI model in which the data is leveraged.

REGULATIONS

Thorough documentation of how data is being collected, stored, transformed and used is not only a pillar of good data ethics but a critical aspect of business strategy to not only improve performance, but also to avoid penalties from regulatory bodies. Regulatory standards should be considered a baseline, to which FIs should be proactive in surpassing to stay ahead of potential ethical or regulatory issues that could arise in the future.

For example, GDPR gives more control to consumers over their data and the processing of it (Directorate-General EU, 2020), while ensuring the individuals behind the data are not identifiable. GDPR serves as a reliable benchmark. However, as we have seen, technology is evolving at such a rapid pace that often regulations have a hard time keeping up. As new technologies

PILLARS FOR ETHICAL DATA MANAGEMENT CONTINUED

become available that facilitate new ways of creating, accessing or leveraging data, FIs must ensure that those applications follow stringent internal standards as regulations may not yet have been developed to the same degree.

FAIRNESS AND RELIABILITY

The proliferation of data across the world is one of the reasons FIs have begun to incorporate AI and machine learning across a wide variety of use cases to minimize human effort and augment human decision making. However, a historical lack of fairness in certain areas can cause a systemic issue in AI and machine learning models if trained on compromised data.

For example, consider the Massachusetts Institute of Technology who recently uncovered a systemic inability for AI to detect early signs of breast cancer in mammogram data from women in minority groups. This stemmed from the fact that these groups historically had less access to healthcare in the United States, resulting in there being far less data representing these groups during the training of the AI models (McGreevey, 2018).

It is important for FIs to be acutely aware of this potential pitfall across all advanced analytics and AI use-cases, however a few key examples include; credit decisioning on loan applications, pre-approval offers, and hiring and human resource decisions. FIs must carefully evaluate the data they are using and examine it for potential bias before training and deploying an AI model on it. This will ensure that models can make decisions without prejudice that can unintentionally lead to discriminatory decisions.

This is especially important to remember if models perform continuous learning. Continuous learning means that information is continuously put into the models as time passes (Lu et al.,2016). The continuous stream of data may cause the model to change over time and can lead to concept drift – meaning the model changes the way outputs are produced, affecting the fairness and consistency of predictions.

PRIVACY AND SECURITY

With the vast amounts of data being generated, stored, and processed, how do FIs ensure it is kept secure and that the privacy of customers, employees, and partners is maintained? The question becomes even more pressing as FIs begin to face regulatory pressures to ensure data assets are being made available to third-party providers from regulations such as PSD2. While at the same time, there has been a rise in number of data breaches of global FIs where large volumes of sensitive, personal consumer data were exposed. As a result, FIs are facing a difficult set of demands; to increase data sharing and openness, while also increasing security.

In order to meet these demands, FIs must establish built for purpose data architectures across their lines of business. Architectural design must provide both a high level of security to personal data while providing the organization with the ability to quickly access, manipulate, and join datasets to extract value from the data. FIs must also accompany architectural design with a clear data governance structure, including data stewardship and data lineage as well as robust master and metadata management. This not only support privacy and security concerns, but the previously discussed pillars as well.

ACCOUNTABILITY

Ensuring FIs remain accountable for ethically managing data and following the previously discussed pillars is not a trivial task. It requires an on-going commitment from the top of the organization. To support this, we suggest FIs do three key activities:

1. Embed data ethics into use-case evaluation frameworks.

2. Establish a centralized Ethics Review Committee to review all use-cases before they move to implementation.

3. Understand how data flows across their organization, and apply the pillars of ethical data management across the data lifecycle.

PILLARS FOR ETHICAL DATA MANAGEMENT CONTINUED

Embedding data ethics criteria into use-case evaluation frameworks forces business decision-makers to consider:

- How they will be transparent with their stakeholders.
- How they will ensure the data is being used and managed in a way that meets regulatory and internal standards.
- If the data to be leveraged in the use-case contains any inherent or unforeseen biases.

This evaluation will help ensure ethical decision making is engrained in use-case selection and prioritization. Establishing a central Ethics Review Committee to evaluate use-cases before going to production alongside the existing business review process will ensure that the use-cases follow an ethical framework. Specifically, for AI models, these reviews should occur at multiple stages from idea generation through data sourcing, model build, validation, and operationalization. Following these steps will help ensure the organization is applying data ethics consistently across lines of business and geographies.

IMPLEMENTING THE PILLARS OF DATA ETHICS ACROSS THE DATA LIFECYCLE

Frameworks can fall short or be short-lived in their implementation as they frequently are not tied directly to the actual day-to-day operational processes. To address this, we have mapped the pillars for ethical data management to the data lifecycle and provided context on how to connect the two.

To begin, let us first level-set on what the data lifecycle is. The diagram below lays out the stages of the data lifecycle. Note that the branches do not apply to all datasets or all organizations. Some organizations may not distribute any data assets for monetization externally. Some may do so with a specific subset of their data assets, while others core business model may center on data distribution and monetization.

DATA ACQUISITION

FIs must be transparent with consumers on what data they collect, how they intend to use it, and how it will be kept safe. FIs must also ensure that the data they are generating or purchasing falls within regulatory guidelines, as well as stringent internal guidelines. FIs should evaluate the data to determine if it provides strategic value to the organization and improves outcomes for customers. If not, it should not be acquired.

FIs should examine if the datasets they generate through business activities or acquire from third parties are subject to a lack of fairness or poses any bias. For example, datasets containing lending decisions can reflect human bias of loan officers that may be discriminatory toward specific groups (Dobbie et al.,2018). Awareness of potential bias can shed light on operations that require changing, and ultimately prevent FIs from making biased decisions through the implementation of advanced analytics or AI models that contain an inherent bias due to the data they were trained on.

DATA STORAGE

Establish the appropriate data architectures across lines of business rather than a 'one-size fits all' approach. Business units generate and acquire different data assets, with differing levels of sensitivity, different intended uses, and different regulatory requirements. The storage mechanism must minimize the risk of a breach (particularly for data that includes sensitive/personal information), while ensuring the organization has the right flexibility and scalability to support data access and aggregation as appropriate.

IMPLEMENTING THE PILLARS OF DATA ETHICS ACROSS THE DATA LIFECYCLE CONTINUED

DATA AGGREGATION

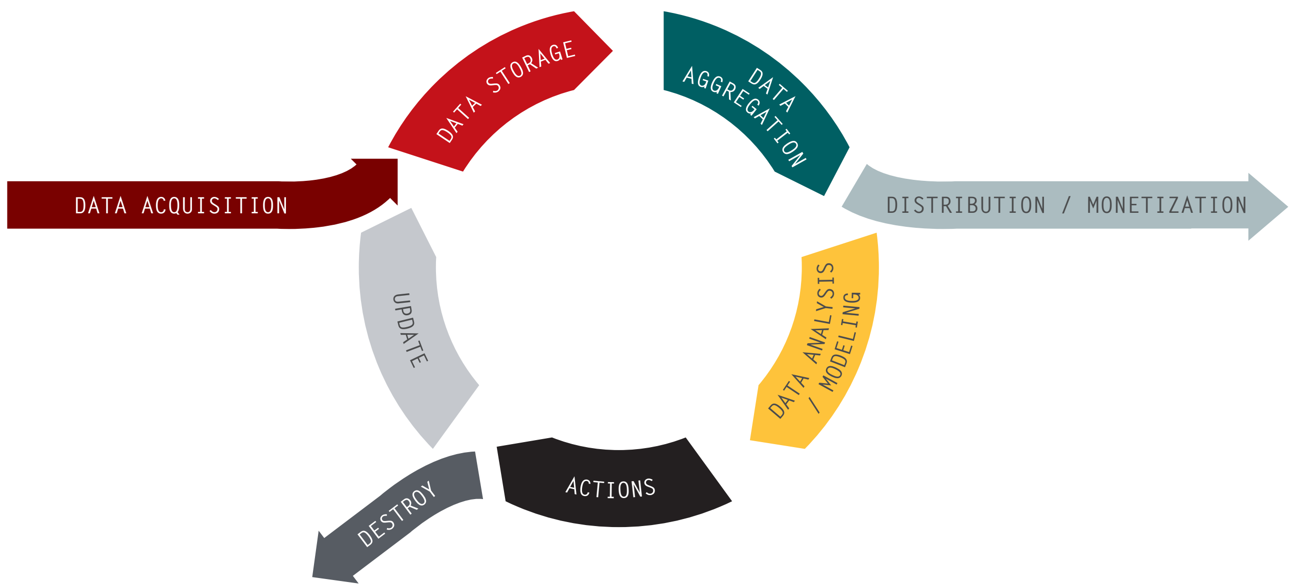
FIs must ensure consumers can be made aware through clear communication how they aggregate and transform their data by processing it, and/or joining it with other data sets that the organization may have purchased or created. Aggregated data sets can allow for masking or removal of personally identifying information; however, they can lead to aggregation bias. Aggregation bias stems from the assumption that a conclusion derived from an aggregated data set applies to all individuals or specific segments within the data set, while the underlying data usually has a distribution across a range. For this reason, FIs need to practice discretion when analyzing aggregated data as it can lead to overgeneralization.

Regulations are often less developed and clear-cut for aggregated data than raw data. However, regulations such as GDPR give more control to consumers over their data, and importantly, the processing of it.

As a result, FIs must have a clear understanding of what unit of measure is appropriate (such as customer, segment, or population) for a given analysis while considering the business question and the distribution of the underlying data to prevent aggregation bias. Further, FIs are required to have a clear step-by-step understanding of how they are processing and aggregating consumer data across the organization, with scalable processes in place to prevent it from happening at an individual level, if requested by the customer.

DATA DISTRIBUTION/MONETIZATION

For organizations that partake in the external distribution and/or monetization of data, they must ensure consumers are aware of this and obtain informed consent before data is collected. Consumers must also be made aware of how the data will be stored, aggregated, and used within both the collecting organization and any that their data will be distributed or sold to. The collecting organization is referred to by GDPR standards as a data controller and is responsible for protecting the rights of the consumer. They must take responsibility to ensure partners (i.e. data processors) meet the same standards from a regulatory perspective and that the data they share will be secured to the same degree by the data processor as in the data controller. GDPR has clearly defined the roles and responsibilities of the data controller and the data processor so FIs can understand their legal obligations when handling the data. Organizations must establish a data processing agreement between the data processor and controller to ensure GDPR compliance from both parties. With regulatory and consumer pressure to make data available, this applies to an increasing number of FIs around the world.



IMPLEMENTING THE PILLARS OF DATA ETHICS ACROSS THE DATA LIFECYCLE CONTINUED

DATA ANALYSIS/MODELING AND ACTIONS

FIs must be transparent with consumers on how their data will be analyzed, and what decisions or actions will be made based as a result of analysis or modeling. Regulatory bodies have certainly had a difficult time keeping up with the advancements in advanced analytics and AI. However, a gut-check FIs should do before putting a model into production, is:

> “*Does this model impact a customer in some way, and if so, can we clearly understand and explain the model results?*”

For example, an FI looking to make credit decisioning should be able to clearly understand their model results, to be able to justify and explain why a decision was made, and to allow them to identify if the data was biased in anyway.

DESTROY AND UPDATE

FIs must be able to communicate to their customers their data retention policies and destruction practices for personal information. Data that is retained will often be updated in several ways, including updates to personal information, changes in purchase patterns, as well as consumer responses to organizational actions taken. Exactly what data will be retained, and for how long, should align clearly to a strategic imperative for the organization, and these practices must fall within regulatory guidelines.

The table below is meant to serve as a guideline for FIs. The pillars for ethical data management should be considered across the full data lifecycle, however, some stages of the data lifecycle require extra consideration from specific pillars.

MAPPING THE PILLARS FOR ETHICAL DATA MANAGEMENT TO THE DATA LIFECYCLE

	Data acquisition	Data storage	Data aggregation	Distribution/ monetization	Data analysis/ modeling	Actions	Destroy	Update
Transparency								
Regulations								
Fairness & reliability								
Privacy and security								
Accountability								

CONCLUSION

The technological landscape is evolving at an increasingly rapid pace, and with it, the volume of data and the opportunities to extract value from that data. However, so is the number of ways in which data can be compromised or misused. Because of this, consumers around the world have become increasingly aware of how important their data can be.

This has created growing public concern around how organizations are collecting, storing, utilizing, and sharing personal data. Although regulators are responding, they have not been able to keep up with the speed of technological innovation. This places the onus on FIs to hold themselves to a higher standard to manage data ethically than the standards that have been set by regulators.

To achieve this, we suggest FIs focus on instilling the pillars of ethical data management across the organization by understanding how each of the pillars connects to different aspects of the lifecycle of data, and use this as a guideline to ensure they ethically manage data.

REFERENCES

Directorate-General. European Union. EU Data Protection Rules. Accessed March 2020.

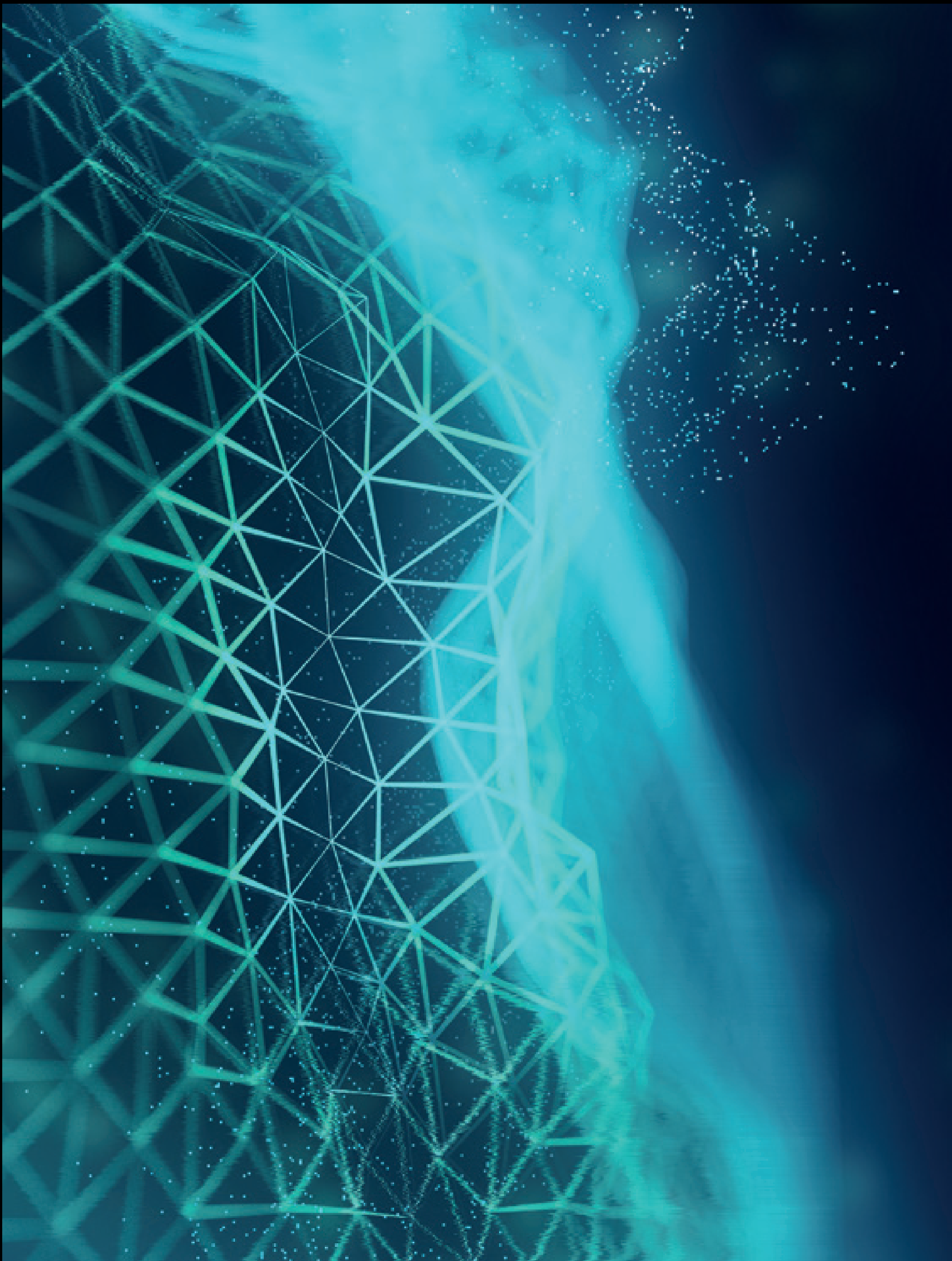
Dobbie, W., Liberman, A., Paravisini, D., & Pathania, V. (2018). Measuring Bias in Consumer Lending.

Lu, N., Lu, J., Zhang, G. & Lopez de Mantaras, R. 2016. A concept drift-tolerant case-base editing technique. Artificial Intelligence.

McGreevey, S. March 7, 2018. Race bias seen in breast-cancer screening. The Harvard Gazette.

Nichols, M. November 15, 2018. Big Data is so large, it's raising privacy & ethical concerns. Euro Scientist.

Kozlowska, I. (2018, April 30). Facebook and Data Privacy in the Age of Cambridge Analytica. Retrieved from https://jsis.washington.edu/news/facebook-data-privacy-age-cambridge-analytica/



EMBRACING THE EVOLUTION OF DIGITAL COLLABORATION IN WEALTH MANAGEMENT

AUTHORS:
Matthew Faraone, US
Phil Kerkel, US
Yola Yu, US

We expect COVID-19 to have a lasting behavioral impact that will accelerate the need for the digitalization of the financial advisor-client relationship. As a result, wealth managers must continue more than ever to pursue forward-looking strategic digital choices despite – and, in many ways, because of – the challenging environment of the COVID-19 crisis to weather the challenge and remain competitive.

As we discussed in our Strategy for Wealth Managers in a Time of Crisis article, in addition to addressing the urgent crisis, financial institutions should prioritize their growth and digital strategy efforts, specifically financial advisor-client digital collaboration. We see the need for this focus not only in the immediate circumstances that define the crisis today but also in what we expect to be long-term and enduring behavioral changes by clients.

Even before the crisis, digital transformation has driven a profound change in the wealth management industry. But, too often, wealth managers have adopted an attitude of a digital-first experience for all clients across all products and the entire service value chain without closely considering the most effective experiences and collaboration models for their client segments.

Part of the reason for this oversight is that Millennial and digital transformation have become nearly synonymous. Wealth managers want to meet Millennials' presumed digital expectations to compete for the great wealth transfer expected over the next few decades. Therefore, many wealth managers embarked on a digital transformation journey, explicitly targeting the Millennial client base – sometimes at the expense of a consistent experience for their current clients.

Now, COVID-19 is putting the past few decades of strategic digital choices to the test. For many wealth managers, the crisis has not only stressed business resiliency and revealed gaps in the operating model, but also shed light on clients' holistic digital experiences. As most current interactions are confined to digital, financial advisors are suddenly challenged to deliver the same quality of service via those digital channels. This, in turn, stresses the demand for different digital collaboration models across client segments.

Our view has always been that digital transformation must allow wealth managers to compete for growing Millennial wealth as well as deepen relationships with their existing client base. Wealth managers need to pointedly invest in appropriate user-driven omni-channel experiences and use flexible and client-focused digital collaboration models to attract Millennial wealth.

As wealth managers begin to transition from crisis management, we are keen to share a few insights, developed through deep user research, on effective foundations for creating a sound and client-centric digital transformation strategy.

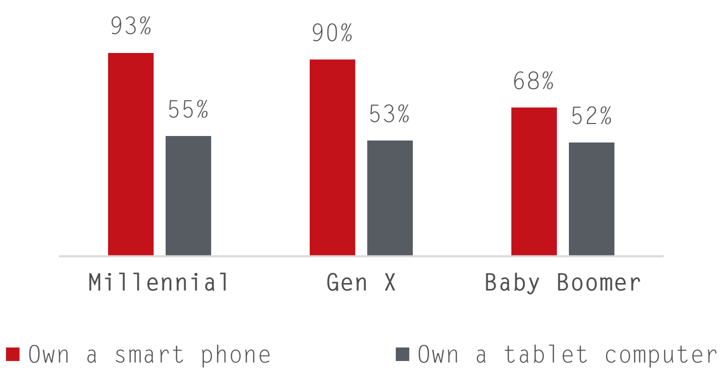
ALL CLIENT SEGMENTS ARE EMBRACING DIGITAL SOLUTIONS

A common misconception is that Baby Boomers and Gen Xers are generally less open to digital technology and solutions. However, research has shown that over 90 percent of Gen Xers own a smartphone, over 53 percent own a tablet computer, and over 86 percent use social media-trends highly comparable to those of Millennials. While relatively lagging, over 50 percent of Baby Boomers own a smartphone or a tablet computer and use social media[1].

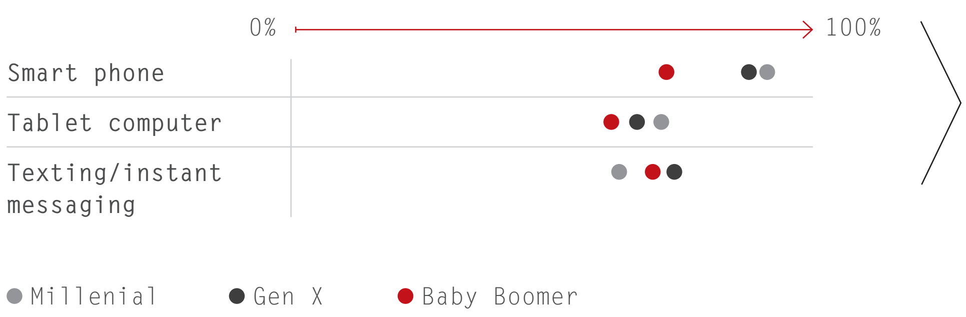
As to wealth management digital solutions, our research and analysis also shows that clients of all generations are willing to adapt to digital solutions that would make their experiences more manageable and consistent across the platform.

As the general population-not just millennials-continues to become more tech-savvy, wealth managers need to be mindful to invest in digital solutions that can flexibly service all client segments.

SMART DEVICE OWNERSHIP



TEXTING / INSTANT MESSAGING



Millennials are comparably less comfortable with texting despite comfort with smart phones

DIGITAL SOLUTIONS SHOULD ENCOURAGE ADOPTION FROM BOOMER & GEN XERS AND PREPARE TO CAPTURE THE MILLENNIAL SEGMENT

While millennials are expected to inherit over $68 trillion[2] from Baby Boomers over the next two decades, it's important to consider that Baby Boomers still account for more than half (57 percent) of the nation's wealth today[3]. In addition, Gen Xers, who account for more than 16 percent of the nation's current wealth and are likely to receive the wealth transfer from Baby Boomers even earlier, are often lost in the fray.

As wealth managers prepare for this wealth transfer over the next two decades, it's important to take a step back to design digital solutions and experiences that will deepen current client relationships. These solutions and experiences should especially cater to current clients (Boomer and Gen Xers), and flexibly reactive to evolving client demands.

WEALTH MANAGERS NEED TO INVEST IN DIGITAL SOLUTIONS THAT SUPPORT FLEXIBLE DIGITAL COLLABORATION MODELS

Digital solutions are not only cutting-edge tools and capabilities from best-in-class vendors but holistic experiences across platforms that best replicate the traditional personal wealth management experience. We have identified four main themes to deliver an optimal digital wealth experience:

1. **Quick access:** Clients expect quick and seamless access to all their information without redundant sign-on or breaks in User-Interface (UI).

2. **Consistency in experience:** Omni-channel access is crucial, but the experience must be consistent across different entry points.

3. **Digital collaboration:** Different segments, even clients within the same segment, expect digital solutions to create different digital collaboration styles, across the wealth management value chain.

4. **Personal services:** Digital solutions and collaboration should not replace in-person access to advisors, but should look to augment the personalized experience for clients.

Quick access and consistency in experience present common pain-points that clients have experienced as wealth managers continue to digitize their services. While digital options are often available to clients across different platforms and products, they often result in disparate experiences. For example, mobile UI is often vastly different from desktop UI, causing user confusion.

In addition, clients are too often required to sign-on in multiple locations or switch platforms several times to view different products and accounts, creating undue burdens.

Digital collaboration reveals the need for wealth managers to remain flexible around their client's digital preferences. Clients often prefer a combination of different digital collaboration models, from in-person interactions enhanced by digital solutions to mobile, desktop, and online bi-directional interactions. These different collaboration models provide impactful opportunities across the wealth management value chain:

WEALTH MANAGERS NEED TO INVEST IN DIGITAL SOLUTIONS THAT SUPPORT FLEXIBLE DIGITAL COLLABORATION MODELS

CONTINUED

Digital solutions are not meant to – and can not – replace personalized services and the in-person wealth management experience. However, digital solutions can supplement and elevate the client experience by reducing inefficiencies to allow for more efficient and impactful financial advisor-client interactions.

	1. Prospecting & sales	**2. Discovery & planning**	**3. Onboarding & client servicing**	**4. Portfolio construction & management**	**5. Practice management & client engagement**
OUR POV	Firms require an advanced **digital sales platform** with capabilities, such as sales demonstration tools, that help **communicate FA value** to prospects, enhanced by **strong CRM integrations and automa ted communications & marketing** distribution	Providing advisors with a **client-centric financial planning platform** equipped with collaborative digital capabilities, maximizes **advisor differentiation** and fosters **strong relationships with end-client**	An **intuitive, AI powered client onboarding portal** with strategic **client engagement opportunities** allows for a seamless user experience and **removes the burden of manual activities** for advisors	Whether building a platform or outsourcing to vendors, **a robust collaboration strategy** is required to allow advisors to **allocate more time to activities that help grow client relationships**	In today's market, **advisor efficiency is paramount** in driving superior firm performance – efficiency can be maximized by **automating advisor activities** and **enabling digital FA/client engagement** capabilities through advanced technology
INDUSTRY INSIGHTS	**Digital sales demonstrations:** Demonstrate value to prospects with demos, such as portfolio back-testing, showcasing how FA's strategies outperform benchmarked portfolios **Data-driven content marketing:** Automated and targeted marketing integrated with CRM solutions to increase prospect pool **Automates sales workflows:** Automated workflows and recommendations expedite sales processes & eliminate manual tasks	**Client-centric financial planning:** A digital platform with interactive capabilities and tools, such as such as digital whiteboarding, co-browsing, and video chats, to provide a holistic financial picture **Innovative goals-based planning:** Advanced planning tools with robust account aggregation and real-time visualization to help clients understand complex concepts **Direct communication:** Expedited communication through secure texting, email, and document sharing	**Optimized UX:** Firms have been using FA/client UX as an opportunity for differentiation as platform capabilities and tools become increasingly commoditized **AI powered digital onboarding:** Lower onboarding transaction time with automated onboarding process **Onboarding due diligence:** Expedite onboarding due diligence process, using secured document sharing, electronic signatures, and other capabilities	**Sophisticated portfolio analytics tools:** Application sharing, whiteboarding, and co-browsing capabilities will allow advisors to effectively communicate their value proposition to the client **Targeted communication:** Increased communication with targeted content through social media, secured texting, emailing, and other marketing tools will help deepen advisor-client relationships	**Enhanced integrations:** Robust integration with CRM and account aggregation systems to maximize utility of insightful client data **Digital engagement:** Enhance collaboration with clients through various digital channels and tools **Automated workflows & next best action:** Machine learning technology and predictive modeling can inform automated workflows and next best action recommendations to maximize FA efficiency and decision-making

WEALTH MANAGERS ARE INVESTING IN A SPECTRUM OF DIGITAL EXPERIENCES

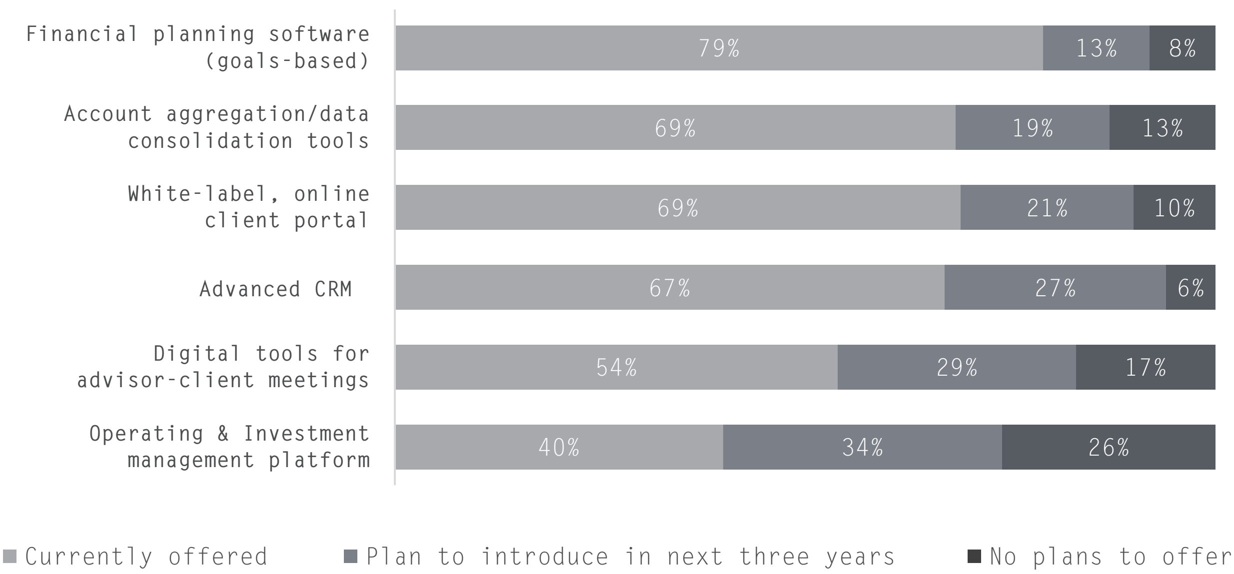
Wealth managers have been investing in a full spectrum of collaboration models, ranging from digitally enhanced in-person experiences to online bi-directional interactions. Some notable recent examples include:

- Wealth managers are modernizing their branches with digital capabilities, such as interactive displays. In addition, advisors often leverage mobile and tablet devices during in-person interactions to create real-time visualizations and sample plans to help clients understand complex concepts.
- To more effectively provide high-touch experiences, some wealth managers are investing in digital capabilities that help simulate in-person experiences for clients, from the comfort of home. These programs leverage portable devices to help financial advisors more efficiently engage with their clients.
- Secure texting capabilities, where clients can send secure text messages to a financial advisor, is becoming a more widespread capability to allow financial advisors to communicate with clients efficiently.

These different collaboration models are designed to leverage digital solutions to enhance and digitally replicate client experience with the advisor, allowing the advisors more opportunities to interact with the clients efficiently.

We at Capco believe it is important to continue to pursue these forward-looking strategic choices during this challenging environment. For the past 20 years, we have helped our clients prepare for and manage such disruptions. And amid the COVID-19 crisis, we remind our clients to take a step back and not lose sight of the big picture – digital transformation will continue to accelerate and, without a targeted digital strategy, wealth managers risk losing clients and financial advisors.

WEALTH MANAGERS' CURRENT TECHNOLOGY AND PLANNED IMPROVEMENTS



Source: Cerulli Associates, US High-Net-Worth and Ultra-High-Net-Worth Markets 2018

REFERENCES

1 https://www.pewresearch.org/fact-tank/2019/09/09/us-generations-technology-use/

2 https://www.cnbc.com/2019/10/21/what-the-68-trillion-great-wealth-transfer-means-for-advisors.html

3 https://www.marketwatch.com/story/this-depressing-chart-shows-the-jaw-dropping-wealth-gap-between-millennials-and-boomers-2019-12-04

LIFE & PENSIONS: A NEW DISTRIBUTION PARADIGM?

AUTHORS:
Rob Wingfield, UK
Alistair Shipp, UK

The life and pensions industry has always been part of wealth management, an activity that all people benefit from. For most workers, their wealth is made up of a combination of deposits and investments and this also includes pension and life policies. In terms of wealth management and financial planning, people have a concept of how to protect their wealth, and that is generally delivered through the sorts of products that life and pensions (L&P) companies provide, and retirement needs especially, which is where L&P providers sit front and centre.

In this article, we share the implications of a potential new trend: life & pensions providers wanting to return to distribution direct to clients, whether that is through direct-to-consumer (D2C) or through their own sales network of advisers. In this increasingly crowded market, it seems that it is not so much the product shelf but rather the distribution side of the industry that is shifting.

> *“Rightly or wrongly, pensions are not seen as a good investment, so providers have work to do to ensure that their customers are aware of fund performance and the level of provision they can currently expect in retirement.”*

FIVE DRIVERS OF INDUSTRY CHANGE

The industry is facing five key external drivers that are influencing the change in distribution of life & pensions services:

1. CUSTOMER DEMOGRAPHICS ARE CHANGING

Today, it is not easy to view your pensions holdings with one company on a mobile device, let alone multiple providers, to see the value of your total pensions pot. This is at odds with the digital direction of travel in financial services, as well as the wants and needs of younger, more tech-savvy, demographics.

Time does not stand still, and as the industry has aged, so have customers. Baby Boomers have mostly retired and members of Generation X are now amongst the oldest in the workforce. This change has meant that Millennials and Generation Z are now the majority of the workforce[1], and the ratio will be ever increasing.

Expectations of how a customer wants to interact with their retirement planning has therefore changed, but the industry has not kept pace. In the wealth management sphere, Hargreaves Lansdown has invested heavily in their digital platform and has reaped the rewards, taking market share from competitors[2]. Other industries have well known examples of household names that have been disrupted and should serve as a serious wake-up call to companies feeling unthreatened by more innovation-focused market players; from Blockbuster, who had the opportunity to buy Netflix at an early stage but ended up being put out of business by them, to Woolworths, who went out of business in the last financial crisis due to online competition by the likes of Amazon, it is clear that no company is safe resting on its laurels.

Increasing customer familiarity with online banking, accelerated during the COVID-19 lockdown, has led to higher expectations of the insurance market - to plan and transact online. The message is clear: younger, digitally native customers expect to be able to transact with service providers at a time of their choosing in a manner of their choosing. Organizations that do not meet that expectation can in turn expect to be disrupted by incumbents investing in such capabilities, or new entrants to the market.

2. PENSIONS HAVE GAINED A BAD NAME

Pensions were once seen as the best and for many, only, way to save for retirement. However, over the last 25 years, we've seen several pensions mis-selling scandals dent confidence in the industry. Closure of company final salary schemes has pushed ownership of investment risk from the employer to the employee and this has coincided with poor performance of pension funds due to low interest rates, the 2008 financial crisis, and now the COVID-19 economic impact. Given the switch to personal responsibility around planning for retirement income, this has led some customers to investigate alternative investments.

Rightly or wrongly, pensions are not seen as a good investment, so providers have work to do to ensure that their customers are aware of fund performance and the level of provision they can currently expect in retirement. Planning for retirement is difficult for customers to understand and pensions terminology can be confusing. Education levels around the suitability of pensions to provide enough income for retirement are low, as is guidance on how to use and make sense of the long-awaited online Pensions Dashboard.[3]

As they get older, Gen Z will gain an expectation of retirement, but what that retirement looks like will likely be different to the traditional view; they may work long past 'normal' retirement age, or work part time while utilising pension draw down or other investments. There is no longer a job for life, so pensions need to be flexible.

3. TECHNOLOGY HAS PROGRESSED… BUT HAVE L&P PROVIDERS?

COVID-19 has accelerated the demand and consumption of digital services across industries. Do providers have the services that customers expect, exposed in a channel they want to use? A 'best of breed' digital capability should include: view and manage personal details, view valuations, view cover details, manage and switch funds, change payments and payment details, change retirement age, model different payment and retirement scenarios, limited funds withdrawal, access documents, education tools to help understand options, and frequently asked questions.

Digitally transforming their businesses should now be an even greater strategic priority for providers, to meet customer demand and to drive value. Learning from the COVID-19 pandemic, it also mitigates the risks of further pandemic-like scenarios to trading and offers the opportunity for insurers to provide new protection products for origination through digital channels.

FIVE DRIVERS OF INDUSTRY CHANGE CONTINUED

Providers have an abundance of data available to them, and many are engaged in programmes to exploit this data, but what tangible difference is this making to customers lives? Personalization of content, communications and product offerings is sparse to non-existent.

Another significant change is the creation of new channels to acquire customers. Two potential sources are the large technology firms and partnerships driven by Open Finance and APIs. Bigtech such as Apple, Google, Amazon and Facebook, have access to billions of users around their world, it is only a matter of time before they create workable technology products allowing their millions of users to purchase insurance from a recognised carrier which has had digital excellence embedded into its products and services from day one.

4. REGULATORS ARE ONCE AGAIN TURNING THEIR ATTENTION TO L&P

After several years of concentrating on the banking sector through initiatives such as Open Banking, regulators are now turning their attention to the rest of the financial services industry, with pensions high on the list of priorities. The aforementioned Pensions Dashboard has been touted for a few years now, and seems likely to be wrapped the consultation on Open Finance. This is a major change which will help younger generations in particular, as the 'gig economy' and auto enrolment will cause the average person to hold a higher number of pensions than ever before.

Millennials and Gen Z will need help to effectively manage their pension portfolios, and the Pensions Dashboard is expected to provide a consistent view of current holdings across all UK providers. Providers will need to ensure that they provide value-added services so that customers will want to use their portal as the place to view all their retirement or investment holdings and plan for retirement. Data aggregation and analysis will allow personalization of the customer experience through this channel and provision of improved financial planning tools, with the additional opportunity to offer consolidation of holdings and upselling. This will also potentially open the way for more regular interactions with customers, enhancing brand loyalty. Typically, L&P customers have little to no interaction with insurers once their pension is set up beyond the requirement for an annual statement until the customer is approaching retirement. This must change.

There have been many delays in getting a Pensions Dashboard off the ground, and whilst there is no reason to doubt that it will eventually appear in some format, there are opportunities for providers to work with fintech and insurtech firms ahead of data being available through the Pensions Dashboard or Open Finance, to offer enhanced retirement planning and modelling tools using user-provided holdings data.

5. RDR BANNED COMMISSION FOR ADVICE… WHERE ARE WE EIGHT YEARS LATER?

Many people do not want to pay for advice and will ask friends, family and Google instead. In addition, due to advice fees, it is often not worth paying for advice for smaller pension holdings unless they can be consolidated – paradoxically, for which it is better to obtain advice. These customers are often left in the dark on their options and need a step-by-step approach.

Since the Retail Distribution Review (RDR) banned commissions for advice in 2013,[4] there has continued to be an advice vacuum that providers have not yet filled. Mortgage providers have offered robo-advice directly to customers for a few years, and Barclays, through their Wealth Management business unit, have recently started to move into this space too, offering robo-advice for those with over £5,000 to invest.[5] For customers who won't use a financial adviser, there is a growing need and opportunity for such a provision, without cannibalising the customer base of their adviser networks.

CHALLENGES AND OPPORTUNITIES

The current high levels of customer queries and transactions will continue as the economy remains volatile. Advisers will not want to take on the burden of being the 'middle man' to such queries and insurer resources will continue to be aligned to service this demand, potentially impacting on other opportunities. Customer service levels may deteriorate as demand exceeds resource available, pulling the focus of leaders to the short term rather than working towards their strategic vision. However, with a direct to customer origination and servicing capability, this effort can be automated digitally, freeing up resource to focus on more value-adding activities.

If the trend of pensions being seen in a bad light continues, contribution to occupational and private pensions will drop to the minimum required under legislation, threatening the retirement provision for millions, and the viability of insurer business models. Providers need to work with the Government and other providers to increase education levels on the benefits of saving into a pension and actively managing retirement investments.

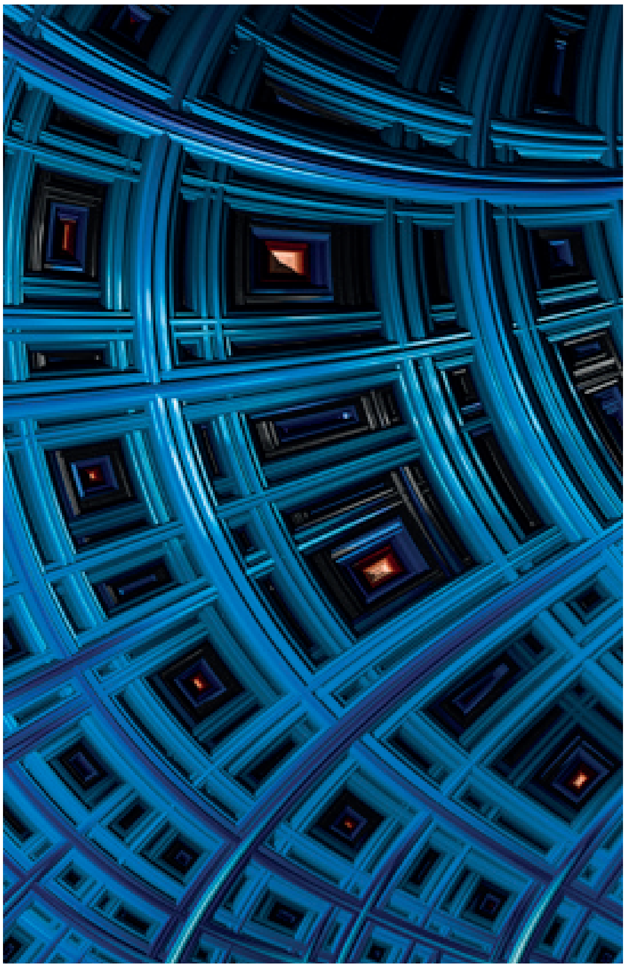
Some providers are already investing in major data transformation programmes. This is a threat to both other insurers, who might be behind the curve in being able to exploit that data to customer benefit and commercial advantage, and to themselves also, especially if those initiatives are not then utilized to provide tangible benefit through personalization of content, communication and product offering. Being able to join this internal data with customer-provided external product holding data and in time, Pensions Dashboard data, will differentiate truly data transformed insurers.

To make the most of these opportunities, insurers will need to tap into expertise that hasn't traditionally been the preserve of the life & pensions industry. Roles should include:

- Customer insight leads to act as customer champions
- Data scientists to exploit internal and external data sources
- Digital proposition designers
- Digital customer journey designers and implementers.

In addition, existing teams will need to re-evaluate their operations which may now no longer be fit for purpose. Going forward, they will need:

- Performance teams to evaluate and optimise the customer journey
- Product specialists to streamline current product and service offerings
- Operational teams (underwriting and admin) to redesign structures and processes
- Leaders to re-orientate the organization to becoming digitally led.



CONCLUSION

The retirement saving sector needs to become increasingly flexible to cater to the expectations of ever younger and more mobile customers. Pensions will be one of the saving mechanisms to achieve retirement ambitions, and insurers urgently need to invest to ensure that the features they need to expose directly to customers can become available ahead of competitors and in line with regulator initiatives such as the Pensions Dashboard and Open Finance.

As the flexibility of retirement saving increases, insurers will need to provide a diversity of savings vehicles, including wealth and asset management offerings, wrapped into a portfolio with accompanying holistic retirement planning and modelling features.

REFERENCES

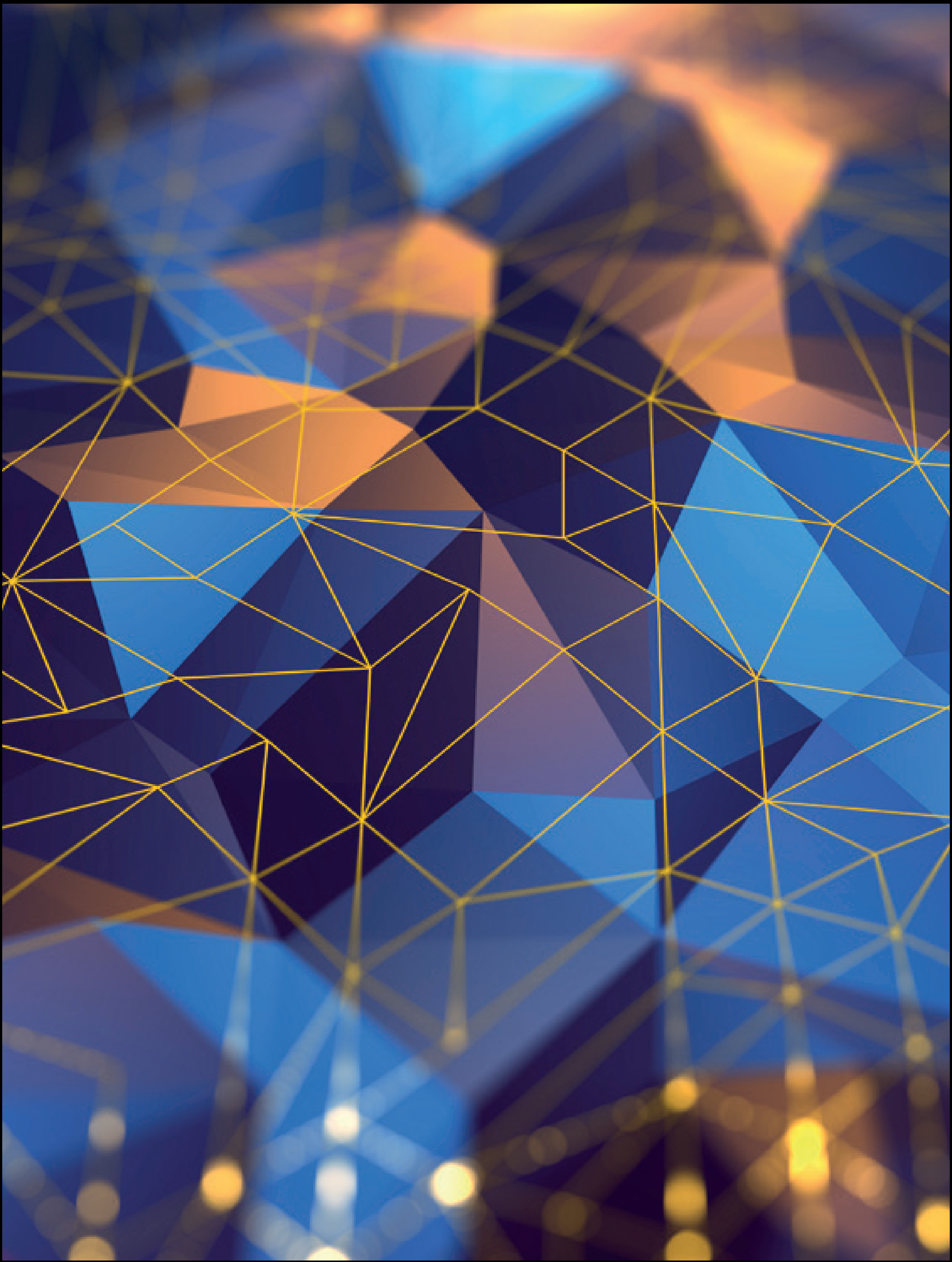
1 https://www.businessleader.co.uk/2020-workforce-to-be-dominated-by-millennials/57878/

2 https://www.directorstalkinterviews.com/hargreaves-lansdown-assets-under-administration-up-5-to-104-billion/412848991

3 https://www.moneymarketing.co.uk/opinion/pensions-dashboard-users-will-need-advisers-to-help-make-sense-of-it/

4 https://www.fca.org.uk/publication/call-for-input/call-for-input-evaluation-rdr-famr.pdf

5 https://www.ftadviser.com/your-industry/2020/07/14/barclays-launches-robo-advice-for-clients-with-5k-to-invest/



DECOMPOSING THE MONOLITH: OPTIMIZATION AND AUTOMATION

AUTHOR:
Gerhardt Scriven, Brazil

We present a data affinity-driven method for decomposing monolith applications into a collection of microservices. The decomposition strategy defined by our process, comprises mapping data objects exposed by the monolith's API endpoints to an enterprise business capability framework and then clustering the business capabilities through data object cohesion. Through this, we define an optimized set of service components that embody business capabilities, but that simultaneously minimizes network latency upon implementation. Using the output from the clustering method, we've developed a strategy that determines where to initiate the decomposition process and how to move from current to target state progressively.

> *"Decomposing a monolith can rarely be done without the underlying code features being enhanced or repaired at the same time. In practice, this often excludes a 'big bang' approach to decomposition."*

INTRODUCTION

A microservices-based architecture enables an enterprise to, through employing multiple teams that work in parallel, deliver business value independently of each other and at greater speeds while collectively avoiding the high cost of ownership that is associated with a monolith architecture[1]. With a well-defined microservices strategy and implementation, you can remove delivery bottlenecks, and develop scalable and resilient software in a manner that is highly responsive to changing business demand, ultimately allowing an organization to embrace BizDevOps practices.

Strategically planning the monolith decomposition roadmap plays a critical role in the success or failure of an enterprise's microservices strategy since:

- A monolith decomposition journey typically co-occurs with the development of new business features as well as the implementation of code patches that address production incidents on the same IT stack. Thus, a key consideration is balancing short and long-term stakeholder expectations regarding the urgency of the transformation within the organization.

- Poor choices surrounding the compositional granularity of the new service layer are hard and costly to reverse. Additionally, it may harm overall system performance and stability.

- For a microservices strategy to genuinely successful, a cultural transformation within an organization that spans well beyond the IT department may often be required[2].

- An important point to consider is that defining a microservices target state is less about the ultimate size of the codebase, but more focused around the logical separation of concerns – specifically data.

You can facilitate a successful decomposition journey by having a target state defined. By doing so, you delineate the future microservices optimally through encapsulating business capabilities,[3] while at the same time ensuring that the overall component composition is not so fine-grained that system performance will suffer when the service layer experiences high demand[4]. This optimized target state will also provide insight as to where to initiate the journey (typically smaller services that have minimal coupling to the rest of the monolith) and how to strangle the monolith systematically.

Our method consists of several techniques that collectively help define this optimal target state and, in the process, identify those features that can easily be decoupled by focusing on data. These techniques, their outputs and the benefits they provide for the enterprise are discussed in this paper.

THE BENEFITS OF BASING THE MICROSERVICES DECOMPOSITION STRATEGY ON A BUSINESS TAXONOMY

Decomposing a monolith can rarely be done without the underlying code features being enhanced or repaired at the same time. In practice, this often excludes a 'big bang' approach to decomposition, and key then is how to systematically distill and release features from the monolith in such a way that business-as-usual project and maintenance work are not adversely affected.

You can attain this by abstracting what the enterprise does in a granular, atomic manner using business-friendly language. In practice, this can be achieved by defining a set of business capabilities and then mapping the monolith against the resultant set. By then defining an orderly manner through which you can release these business capabilities, one by association also defined the decomposition path for the monolith. However, the key to the end-to-end undertaking is also understanding the cohesion/ lack of cohesion among the business functions as this knowledge will help one avoid making the service stack too granular.

Furthermore, you may describe a long-running workflow (such as selling a product/service to a new client) through a collection of business capabilities being triggered in sequence and/or parallel. Such a workflow thus represents a vehicle through which you can realize several business capabilities collectively to achieve a larger goal. In a technical implementation, a workflow orchestration engine can embody this business process workflow by executing microservices that each, in turn, aligns directly to a business capability. The approach thus helps align Product with IT more closely.

A collection of business capabilities that are structured logically in a hierarchy form a business taxonomy. Industry-standard business taxonomy frameworks do exist, such as the business process framework (eTOM) for the telecommunications industry, and the banking industry architecture network (BIAN).

When applying our method, an enterprise may choose to adopt such an industry framework, implement a derivation of one, or created a business taxonomy from first principles.

In the latter case, the taxonomy could potentially be defined through internal consultation and will most likely comprise of a functional view of the organization:

Sales | Contracting | Sign Contract,
Billing | Bill Calc | Calculate Taxes, etc.

Alternatively, the taxonomy may arise organically (bottom-up approach) by evaluating and abstracting details captured in existing technical models that describe the organization's business and IT processes (business modeling process flows, sequence diagrams, use cases, etc.). This bottom-up approach holds several advantages over predefining the functional taxonomy. These advantages include speed of analysis (significantly less time is needed for consulting activities), and avoiding the creation of artificial functional silos (with the corresponding duplication of data and associated synchronization related concerns). However, the process demands enterprise maturity in documenting their business and IT processes.

Cardinal to the custom approach, is that the taxonomy should ensure close alignment with key business concepts and language used within the enterprise to align business and IT better. Moreover, each business capability:

- Should be atomic, i.e. it provides a small, repeatable business-centric outcome.
- Usable across many different workflows. Workflows employ one or more capabilities to execute a long-running process, and typically provide more significant business value (such as customer onboarding).
- Optionally creates, modifies, or references data as part of the atomic task that it performs. Note that the data it creates, modifies, or references may potentially be owned by a different business capability.

Also note that while business capabilities are atomic and independent, they share an indirect connection through common data objects. A data object represents data at a macro or business level (i.e., the collective concept of the customer's billing address as opposed to the customer billing address postal code.). A data object may be conceptually viewed as a data clustering or hierarchy, which is distinct from the business capability hierarchy. Data objects may be shared among several services. As a

THE BENEFITS OF BASING THE MICROSERVICES DECOMPOSITION STRATEGY ON A BUSINESS TAXONOMY CONTINUED

simple example, a customer's address can be used by a CRM related service to capture the underlying information. Later, a tax calculation service could use that information to determine appropriate taxation based on location. Lastly, an invoice generation service could use the information to decide which address the customer invoice will be sent.

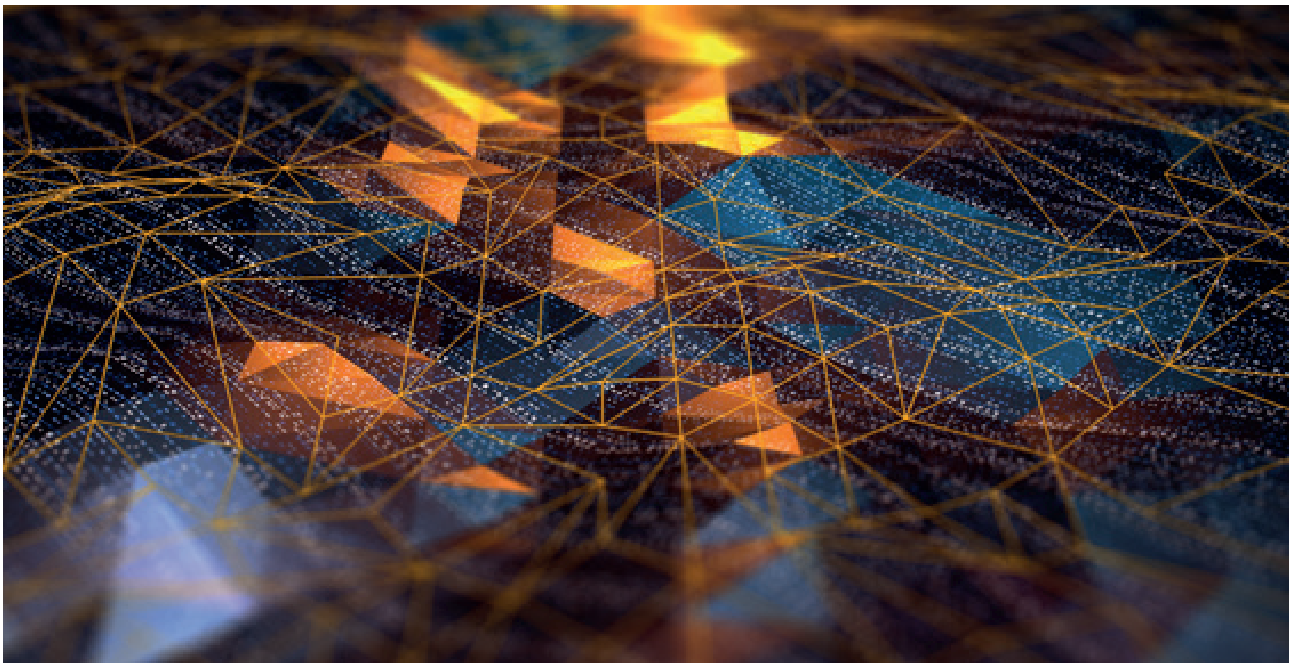
Data objects play a cardinal role in determining how to cluster business capabilities into an optimized services stack.

As a simple example, consider a business capability taxonomy that has distinct entities for creating a contract with the customer, having the customer sign the contract, and having the organization countersign the same contract. One could theoretically create a microservices target state where each of these three atomic capabilities aligns directly with a dedicated microservice. However, the better solution may be to cluster the three capabilities into a single microservice simply because they will all use the same data objects to achieve their respective outcomes. By using the single microservice approach, you still preserve the concept of business to IT transparency. Still, you will reduce overall network traffic will during implementation as the three functions will, for the most part, feed off data stored in their common service database, as opposed to needing to query across services. It also helps resolve the issue of data ownership, i.e., to which service does the physical implementation of the client contract data object belong to.

As a final note to the question of the granularity that business capabilities should be defined when defining a custom taxonomy. For monolith decomposition, the choices made are tolerant to under/oversizing. This is because:

- Capabilities that were defined too granular will eventually cluster together, as will be discussed in the section on Optimizing

- Capabilities that were defined at a level that is not granular enough will ultimately reveal themselves as being associated with too many data objects (using the method that we describe in the next section). In these cases, you should decompose the business capability into two or more capabilities of greater atomicity.



MAPPING MONOLITH BUSINESS CAPABILITIES TO DATA OBJECTS

As we previously mentioned, the method we describe requires knowledge of the association between data objects and business capabilities. Because a microservice essentially is a combination of business functions, data needed by the functions, and API endpoints through which the functions can be executed and/or create, retrieve, update and delete (CRUD) operations on the data may be performed.

As a proof-of-concept, a subset of customer journeys, collectively forming a new initiative for one of our clients, was used to define a custom taxonomy from first principles as part of a pilot project. The taxonomy was defined and refined along with seven key activities:

1. **Identifying all the long-running workflows by analyzing business process models** as well as app (Android/iOS) screen flo w mock-ups and business-level requirements for the initiative. The resultant dataset became the primary dimension of the taxonomy analysis.

2. **Defining business capabilities referenced inside the business process models and app screen flows by analyzing activities and generating abstractions.** For example, a set of activities inside a logic branch in a Business Process Model (BPM) may pertain to obtaining user personal information, and others may pertain to obtaining a client's account balance. These abstractions, when defined granular

WORKFLOWS | BUSINESS CAPABILITIES	UPLOAD PROOF OF RESIDENCE	...	SEND NOTIFICATION	OBTAIN ACCOUNT BALANCE
Account management				
…				
…				
Change mobile device				
…				
…				
…				
…				
Reset password				
…				
…				
…				
…				
Onboard customer to digital platform				

Figure 1. Partial cross-map of workflows to business capabilities (note that some data has been masked)

MAPPING MONOLITH BUSINESS CAPABILITIES TO DATA OBJECTS CONTINUED

and atomic as described previously, are the business capabilities, and form the secondary dimension of the taxonomy analysis. Note that business capabilities are conceptually usable across several different workflows. As an example, the business capability “lookup account balance” is shared among “make an investment” and “transfer money to a different account” workflows, even though the actual underlying implementation of the business capability may potentially be different among the workflows.

3. **Cross-mapping the workflows that were identified to the business capabilities that were defined to lock down the main taxonomy structure.** This step plots the correlation between the primary and secondary dimensions referenced above (points one and two) and becomes the platform through which you perform the rest of the analysis. A conceptual and partial example of this is shown in Figure 1 based on work done for the pilot project. Note that the collection of activated business capabilities for any given workflow fully covers all aspects of that workflow, but that no sequence of business capability invocation is implied.

4. **Aligning client app screens to the business capabilities for each workflow as part of an IT enabler deep dive.** For our pilot, we had access to approximately 200 app screen mock-ups and associated logical flows. Each app screen mock-up was cross-referenced to the appropriate workflow/business capability cluster.

5. **Identifying and mapping which API endpoints are invoked for each app screen.** In addition to business process models and app screen mock-ups and flows, we also had access to Unified Modeling Language (UML) sequence diagrams that describe the detailed execution of core aspects of the workflows. This allowed us to correlate app screens to API endpoints, and then to use this association to cross-reference the API endpoints to the taxonomy.

6. **Extracting data objects from each referenced API endpoint by analyzing its specification.** For our pilot, this exercise was relatively trivial as all the APIs are RESTful, and each endpoint references a single data object. This may not always be the case: In practice, APIs may contain

DATA OBJECT | BUSINESS CAPABILITIES	UPLOAD PROOF OF RESIDENCE	…	SEND NOTIFICATION	OBTAIN ACCOUNT BALANCE
Client				
…				
Account				
Mobile device				
…				
…				
…				

Figure 2. Partial cross-map of data objects to business capabilities (note that some of the data had been masked)

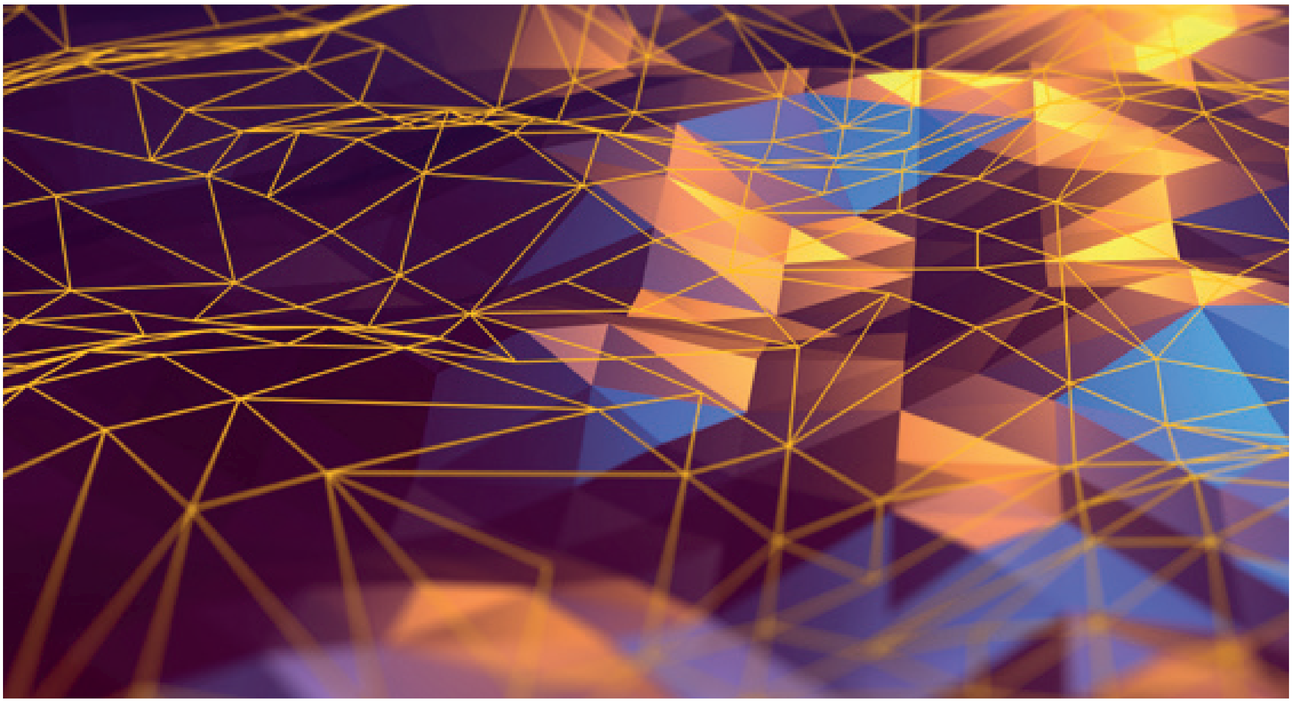
MAPPING MONOLITH BUSINESS CAPABILITIES TO DATA OBJECTS CONTINUED

hundreds of data elements that may roll up to several data objects. In these instances, we recommend that automation around extracting data objects from the API specifications or underlying code is embraced.

7. **Once the data objects were extracted from the API endpoints, they were cross-mapped to the taxonomy through inference to the API endpoints that had already been mapped (see step six).** At this stage, a new view of the taxonomy can be generated by illustrating the correlation between business capabilities and data objects. This is depicted in Figure 2 for a partial subset of data derived as part of the pilot project. As can be seen in Figure 2, each business capability references one or more data objects. The collection of data objects that are associated with any given business capability is then that capability's data object thumbprint.

There is a good strategy for if any business capability appears to be overloaded with data objects, and if (and only if) these data objects are not pushed to the function. The strategy features re-evaluating the capability to determine whether you can split it into two or more capabilities of greater granularity since comparing the capability as is with any other capability will probably result in low cohesion results. To illustrate this, note that the 'Send Notification' capability in Figure 2 is associated with several data objects. However, the majority of data objects, such as account and device, are pushed to the function (the function does not pull the data as part of sending notifications), and hence there is no need to split the function. However, had this data been pulled by the 'Send Notification' function, we would likely have split the capability into more atomic functions before continuing with the remainder of the analysis.

Now that we've defined the business capabilities, and each has been associated with one or more data objects, the next analytical step is to cluster the capabilities through their mutual data affinity.



OPTIMIZING THE SERVICE STACK THROUGH CLUSTERING TECHNIQUES

Two clustering methods were independently used to group the business functions based on data affinity: cosine similarity analysis, and k-means. The results from the two methods were compared, and a recommendation is made around the most appropriate technique for this particular problem domain.

COSINE SIMILARITY

When using cosine similarity measurements, the cohesion among the various business capabilities can then be expressed as numbers with values residing between 0 and 1. This allows one to define (or, if needed, redefine) a threshold value which will drive the granularity and relative size of the clusters.

In practice, the collection of data objects that had been associated with each business capability is vectorized using a one-hot encoding approach, and a cosine similarity value is then calculated to determine the cohesion, or lack thereof, among the entire set of capabilities. Figure 3 conceptually illustrates how the data objects are vectorized for each business capability using one-hot encoding.

Note that the cosine similarity formula (see Figure 4) uses the dot product between, and magnitude of, the two vectors in question, and neither will be affected by the specific ordering of the dimensions that represent a data object in the set of vectors.

Business capabilities	**Data object vector**				
Business capability 1	1	0	1	…	1
Business capability 2	0	1	1	…	0
Business capability 3	1	0	0	…	1
…	…	…	…	…	…
Business capability n	0	1	0	…	0

Figure 3. Vectorization of Data Objects by Business Capability. A value of 1 in the vector representation represents the fact that a business capability references a particular data object (such as account). In contrast, a value of 0 denotes that that capability does not reference that data object.

$$\text{similarity} = \cos\theta = \frac{A.B}{||A||\,||B||} = \frac{\sum_{i=1}^{n} A_i B_i}{\sqrt{\sum_{i=1}^{n} A_i^2}\ \sqrt{\sum_{i=1}^{n} B_i^2}}$$

Figure 4. Cosine similarity formula where A and B represent two vectors[4]. Within the context of this discussion, A and B thus represents the data object composition (thumbprint) of any two business capabilities in the taxonomy we defined.

OPTIMIZING THE SERVICE STACK THROUGH CLUSTERING TECHNIQUES CONTINUED

Calculating the cosine similarity among all business capabilities will yield a matrix, as is shown in Figure 5.

In the matrix, values closer to 1 show a relatively high cohesion between the two business capabilities, and these are candidates for clustering together. Examples in Figure 5, illustrated with the circles in the matrix, include business capabilities one and three, as well as business capabilities two and n.

Conversely, values closer to 0 show little cohesion between two business capabilities, and they should logically not be clustered. Moreover, a business capability that has low cohesion to all other capabilities, as is the case for business capability (n-1) in Figure 5, can be completely isolated. These capabilities are excellent candidates for starting the microservices journey.

As part of this method, a cohesion threshold value should be chosen where cosine similarity values are greater than the threshold drives when business capabilities should be clustered. Depending on this threshold choice, clusters will logically be larger or smaller, but regardless, these clusters define target state microservice candidates.

Alternatively, the clustering process could be repeated recursively until all cosine similarity measurements among clusters have relatively low values and that no new clusters can logically be formed. Each supercluster that is derived through this process will be a target state microservice. This is illustrated in Figure 6 that shows how each microservice candidate, through tracing to the hierarchy, is still directly aligned with a business capability.

Ultimately, our method provides for an optimized set of services that encapsulate granular business functions as best practice but are balanced at the same time by defining a minimal set of physical components in the services stack, which will help ensure improved network latency.

TAXONOMY	BC 1	BC 2	BC 3	...	BC N-1	BC N
BC 1	1	0.5	0.95	...	0	0.65
BC 2	-	1	0.35	...	0.01	0.90
BC 3	-	-	1	...	0.025	0.40
...	-	-	-	1	0.03	0.33
BC n-1	-	-	-	-	1	0.02
BC n	-	-	-	-	-	1

Shows high cohesion and hence capabilities that may be clustered. Clusters become candidate μSs.

A capability that is highly isolated and can as a result easily be lifted out of the monolith as a stand-alone μS.

Figure 5. Business capability similarity matrix.

OPTIMIZING THE SERVICE STACK THROUGH CLUSTERING TECHNIQUES CONTINUED

K-MEANS CLUSTERING

Complementary to the Cosine analysis, the business capabilities were also clustered using the k-means method. Here, the same one-hot encoding values were used to represent the data object thumbprints for each of the business functions. A simple Python script was used to execute the algorithm, selecting the same number of output clusters as what cosine similarity analysis naturally revealed.

The clusters that resulted from executing the k-means script had approximately 75 percent direct correlation with that of the Cosine Similarity analysis. The main concern with using k-means as opposed to cosine similarity, (which requires more manual work) is that the algorithm has no context about the business capabilities themselves. So when clustering, it would, in some cases, lump business capabilities together that ideally should functionally be separated as they represent very different business domains. Accounting for most of the deltas between the two clustering methods. Note that k-means is known to have trouble clustering data where clusters are of varying sizes and density[6], which is certainly the case in this dataset.

As a result, while k-means certainly could be used to create a first approximation of the clusters, the cosine similarity approach allowed for greater control, and hence a more contextually relevant grouping of business capabilities, at the cost of more human involvement.

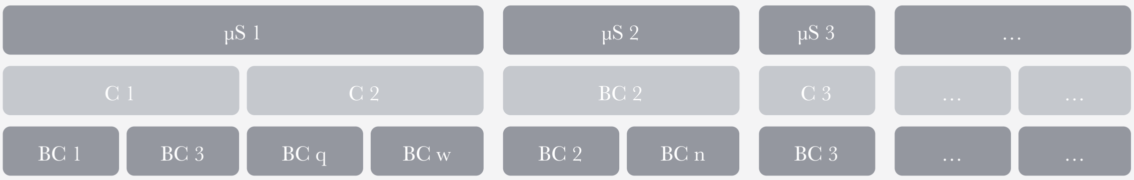


Figure 6. Visualization of a target state microservice architecture that is derived through recursive clustering.

	DATA OBJECT 1	DATA OBJECT 2	DATA OBJECT 3	...	DATA OBJECT N
µS 1	✓		✓	✓	✓
µS 2		✓	✓		
µS 3				✓	
...	...	...	...	...	...
µS y	...	...	...	...	...

Figure 7. Some data objects may be required by more than one microservice.

OPTIMIZING THE SERVICE STACK THROUGH CLUSTERING TECHNIQUES CONTINUED

DATA OWNERSHIP

After clustering, there may be cases where data ownership needs to be resolved as it will often be unavoidable that a subset of target microservice will need to operate on the same data object(s). This is illustrated in Figure 7, where the data object composition has been rolled up to a microservices view.

For example, in Figure 7, microservices one and two have a shared need for access to data object 3.

In these instances, a set of rules are defined to determine which microservice will own the data tables and API layer that provides access to the data underlying the common data object. These are, in order of importance:

1. Whether the business capability pulls the data or whether it is pushed towards it (such as in a notification service). When data is pushed towards it in the legacy system, the associated microservice will logically not be a candidate for ownership

2. Which function updates the data object more frequently

3. Which function consults the data object more frequently

Putting this in practice, Table 1 shows a partial result from the project on which we piloted the method. The type of view illustrated in Table 1 will help define a decomposition roadmap.

TABLE 1

THE PARTIAL RESULT FROM CLUSTERING AND DATA ASSIGNMENT ANALYSIS FOR THE PROJECT ON WHICH WE PILOTED THE DECOMPOSITION APPROACH.

MICROSERVICE	CONTAINS BUSINESS CAPABILITIES	DATA OBJECTS OWNED	DATA OBJECTS OWNED	DECOMPOSITION PRIORITY	CONSUMES
CustomerService	Onboard customer Change profile …	Client device …	Account	4	AccountService InformationService
AccountService	Obtain account balance transfer …	Account credit …	Client …	3	CustomerService NotificationService
NotificationService	Send notification cancel notification …	Notification	Device client	1	None
InformationService	… …	… …	… …	2	None

CREATING A DECOMPOSITION ROADMAP

With the clustering exercise completed, a roadmap can be defined whereby clusters that can be decoupled from the monolith readily (due to low cohesion to any other clusters) are prioritized. This approach will also provide development teams the opportunity to validate and fine-tune development, testing and deployment strategies and best practices. All of which ensures the infrastructure serves the stated need (including potential data synchronization with the monolith legacy database), that non-functional requirements (performance and security) are satisfied, and that business-as-usual delivery of new business features are not impacted negatively.

Once delivery execution has matured for the first handful of microservices, a decomposition release train for the other services can be established. To construct the path of execution, we recommend decomposing, as far as possible, around those functional clusters in the business taxonomy where work intake will already occur for a given sprint. For example, if taxation rules need to change as part of the prioritized backlog for a given sprint, the corresponding business capabilities that roll up to the microservice that align to this should ideally be targeted for decomposition around the same time. In this way, stability around the rest of the IT ecosystem can be assured while optimizing the use of development, test, and project management resources.

An implementation strategy for this recommendation is as follows (assuming functional work will occur on a business capability cluster in sprint n – see Figure 8 for reference):

- Lift-and-shift the existing monolith code that corresponds to the targeted (clustered) business functions during the sprint (n-1) and regression test over this period. The code reorganization includes moving corresponding data structures, data synchronization with the legacy database, API endpoint locations, etc. Note that the API endpoint and data structure definitions should remain unchanged to ensure the stability of the greater code base, but that minor refactoring may occur (such as moving business rules to a dedicated rules-engine or to resolve technical debt). The new code base also needs to adhere to non-functional specifications that were established for microservices within the enterprise. This includes security, logging, availability, performance-related SLAs, etc., as well as to other enterprise architecture related mandates.

  At this stage, the monolith will still contain the original function call signatures (to ensure that the consumers are not impacted). Still, it will forward such calls to the new microservice and return the results to the calling consumer. Moreover, all internal monolith calls that accessed the original set of CRUD related API endpoints need to be refreshed to point to the new location/version.

- During sprint n, new business features (based on functional work intake) are added to the microservice. APIs and Data structures of the microservice may change to accommodate the new/changed features. Signatures in the monolith's forwarding calls, as well as the monolith data structures, may need to be updated as a result. Consequently, consumers calling into the monolith may need to update their codebase to account for such changes.

  Additionally, appropriate workflows will be added to the orchestration service layer (assuming an orchestration approach is followed). Still, it will not yet be wired up to the monolith and microservices collection for general consumption (but may be tested as part of a controlled introduction deployment strategy).

- During sprint (n+1), client calls will be routed to the orchestration service for general consumption, and comprehensive regression testing will be conducted.

CREATING A DECOMPOSITION ROADMAP CONTINUED

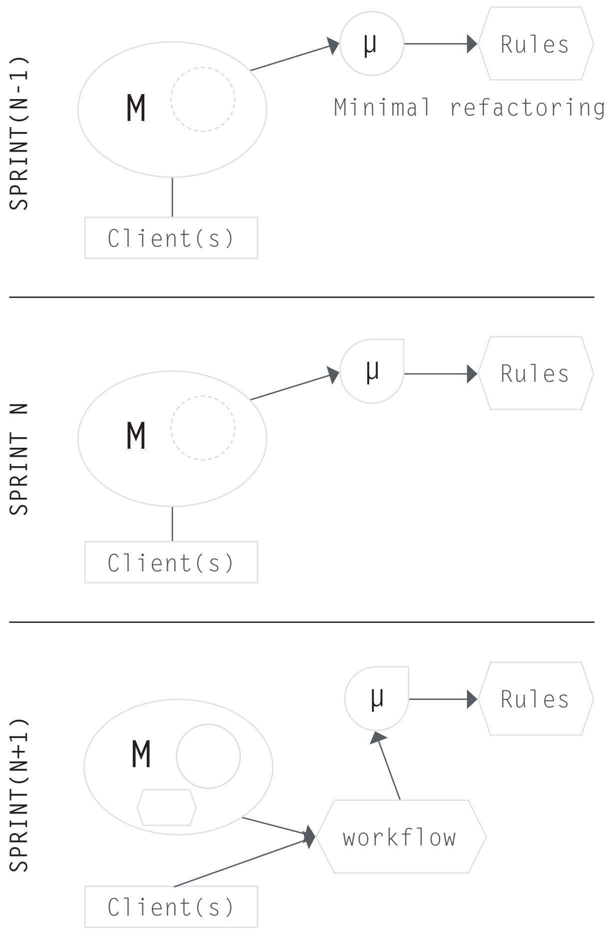


Figure 8. The recommended decomposition strategy spread across three sprints.

MANAGING NEW BUSINESS FUNCTIONALITY

After the microservices initiative is complete, or even while it is in flight, it is expected that new business features will need IT enablement as part of standard IT project work. The question is whether such new features should be added as new services in the microservices stack or whether existing services should be extended.

The same clustering method that was used for slicing the monolith, can now be reused to help with these decisions via knowledge of the data object thumbprint for each microservice. This implies that data object thumbprint information should be maintained for the collection of microservices.

The new business feature is then analyzed in terms of its own data object needs, and its data object thumbprint is subsequently determined. Using the exact same method as was described earlier, the affinity between the new business feature and the existing microservices are determined. Based on the findings, either a new service is proposed, or one or more of the existing microservices are extended to encapsulate the new feature.

OTHER BENEFITS OF MAPPING THE BUSINESS TAXONOMY TO THE MICROSERVICES STACK

As well as defining a monolith decomposition strategy, there are several other benefits in employing a business capability taxonomy in an enterprise. Some of these benefits can help the enterprise on its journey towards establishing BizDevOps practices, others can provide strategic insight for optimizing operational improvement initiatives. A few examples are listed below in Table 2.

TABLE 2

SHORT AND LONG-TERM BENEFITS OF EMPLOYING A BUSINESS CAPABILITY TAXONOMY

REALIZATION	BENEFIT
Short term	• It helps with scrum teams functional collision detection early in the software development lifecycle. By mapping work intake to business capabilities for each project/scrum team, an early readout can be obtained about inter-team dependencies, which, in turn, allows for more effective project management and potentially avoiding complex code merge issues by ensuring the work execution occurs in different sprints. • Helps architects systematically analyze which IT components are impacted, i.e., which monolith classes and/or microservices will need to be changed based on new work intake. Furthermore, when a specific business capability is determined to be impacted, the data objects associated with this capability are analyzed for structural impact (example, street name field length needs to be increased from 30 to 50 characters). The knowledge thereof drives secondary business capability impact analysis as data objects are often shared among business capabilities. • Helps test analysis systematically where new work extends existing features. This can significantly facilitate regression test analysis if the additional effort is taken to map the taxonomy to test cases.
Medium/long term	• Helps mapping of enterprise project issues, test defects and production tickets to the business capability framework and quantitatively highlight where process optimization will yield the best ROI. Assuming a defect can be traced to a microservice or API endpoint, for example, following the breadcrumb trail will lead to an impacted business capability. Through analysis of many defects and incidents, patterns will emerge that can provide an enterprise with data-driven insight around which business capabilities are the most troubled. Following the Pareto 80/20 rule, that small subset of business capabilities that collectively cause the most harm to the enterprise can consequently be isolated and analyzed for areas of improvement and re-engineering. • Predictive models via cognitive automation: Historical data around specific inputs and associated outcomes can be mapped to the business capability framework and used to train cognitive models that in turn can, via mapping of new work intake to the same taxonomy, be used to predict outcomes (e.g., whether the project will result in budget overruns, etc.).

EVOLVING THE METHOD

While the method yielded very satisfactory results for the pilot that was conducted, two areas were identified that would require further thought and analysis to accelerate its adoption as a standard practice. These are:

- **Mining information needed to build the taxonomy:** For the pilot, we had a very well documented business process models, App screen flows, UML Sequence Diagrams, and API specifications at our disposal – there was little to do in terms of mining the information, and the details were sufficient to construct the business taxonomy largely independently. This will not always be the case as one may be in a situation where the legacy system(s) were created 2 or 3 decades ago, and documentation is outdated or missing, and/or subject matter experts left the enterprise. In a scenario such as this, it would be helpful to have a tool that can automatically / semi-automatically mine the information needed to build out the taxonomy by scanning the underlying legacy codebase.

- **Automation in extracting data objects from API specifications and/or code:** In our pilot, APIs were RESTful, and well documented. Moreover, we only had approximately 50 API endpoints to analyze. As a result, extracting data objects was a trivial exercise for the pilot. However, in the case where there may be thousands of poorly documented APIs and where multiple data objects may be transported through the endpoints, human labor will be an inefficient way of extracting the required information. Automation, possibly through applying machine learning techniques, may be highly valuable to reduce the amount of labor needed to perform this critical task accurately.

CONCLUSION

An optimized decomposition strategy of a monolith to a collection of microservices, can be derived through the adoption of an appropriate business taxonomy, the alignment thereof to legacy IT constructs, and clustering business capabilities in the taxonomy by means of data object affinity.

The approach outlined here is not only a once-off exercise. As the enterprise business evolves its products and services over time, and expresses this evolution via IT enhancements, the exact same technique can be used to package new functions and data in appropriate service containers – i.e., the method will recommend whether such IT functions and data belong in new microservices or whether one or more of the existing services should be enhanced. This way, a consistent, repeatable, and measurable approach to IT evolution, and that has good alignment with the product, can be established and maintained.

Moreover, while the approach described was focused on decomposing a single monolith, the approach outlined is equally valid for a distributed IT environment with several monolithic applications. Specifically, secondary and tertiary monolith applications' decomposition components can be compared to the microservices that were derived from decomposing the first monolith using the same approach. In this way, duplication of business features and data can be avoided by making enhancements to established microservices where there are areas of functionality overlap.

Key to the analysis is selecting or defining a business taxonomy that has the appropriate level of granularity. Moreover, the business functional taxonomy becomes a cornerstone against which many other IT related activities can be performed, including requirements and architectural analysis, regression testing needs, as well for providing as deep data driven insight into an enterprise's most troubled operations.

REFERENCES

[1] Fachat, André. Challenges and benefits of the microservice architectural style, Part 1, 2019,
Web Page: https://developer.ibm.com/technologies/microservices/articles/challenges-and-benefits-of-the-microservice-architectural-style-part-1/

[2] Kozłowski, Albert. How Microservices Architecture Impacted the Culture of Software Development, 2019,
Web Page: https://medium.com/better-programming/how-microservices-architecture-impacted-the-culture-of-software-development-6bba363ecdf1

[3] Lewis, James. Microservices, a definition of this new architectural term, 2014,
Web Page: https://martinfowler.com/articles/microservices.html

[4] Laskowski, Dave. Moving to Microservices: How Granular Should My Services Be?, 2019,
Web Page: https://tcblog.protiviti.com/2019/09/04/moving-to-microservices-how-granular-should-my-services-be/

[5] Prabhakaran, Selva. Cosine Similarity – Understanding the math and how it works (with python codes), 2018,
Web Page: https://www.machinelearningplus.com/nlp/cosine-similarity/

[6] Yordan P. Raykov, et al. What to Do When K-Means Clustering Fails: A Simple yet Principled Alternative Algorithm, 2016,
Web Page: https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0162259

ESSENTIAL SUCCESS FACTORS IN LAUNCHING A FEE-BASED CLIENT ADVISORY

AUTHORS:
Warren Li, Singapore
Neal Kirk, Singapore

Private banks face challenges on multiple fronts in the form of flat revenue growth, falling margins, and client defections to banks with better digital footprints. Even more pressingly, declining levels of client activity and changing investment attitudes threaten the traditional business model of private banking.

Many banks have been looking to reverse this trend by offering differentiated service models. While fee-based advisory service offerings have been available in the market for clients, they were mainly offered by boutique investment advisors. During the decade after the financial crisis, several large bulge bracket banks in Switzerland started offering such services. Other international and regional private banks have followed suit, rolling out their own versions of fee-based advisory.

So, given the myriad features, pricing models and client benefits offered by different banks, what constitutes the essential elements for this advisory model to succeed?

> *“Clients view investment ideas as a value-add and possibly complementary to their own, but are often suspicious of hidden product commissions.”*

SINGLE ALL-IN FEE SCHEDULE

The prevailing private banking advisory model remains based on transactional advisory, especially in Asia and other emerging markets. While advice is marketed as free to clients, the cost of that advice is bundled together in the products that are subsequently sold to the clients. As a result, clients view investment ideas as a value-add and possibly complementary to their own, but are often suspicious of hidden product commissions.

In a fee-based advisory model, private banks can achieve the goal of unifying advice and products under a single fee schedule. With a clear all-in fee schedule, investment advice and products are perceived by clients as one unified service. Clients are more inclined to accept the service without having to worry about potential conflicts between free advice and commission-based products.

TRANSACTIONAL ADVISORY	
Free service:	• Advice • Investment ideas • Portfolio reports
Clients pay transactions:	• Product commissions • Trading spread • Tax and duties • Banking services • Custody services

ALL-IN FEE BASED ADVISORY	
Single and all-in fee:	• Advice • Investment ideas • Portfolio reports • Banking services • Custody services • No product commission • No trading spread • Absorbed taxes and duties

PRICING TRANSPARENCY

Since the 2008 financial crisis, clients' distrust toward complex investment products has grown due to obscure costs hidden within the price of products. The perceived lack of transparency in the commission structure of the traditional transactional advisory, and the misalignment of incentives between advisors and clients, has raised the question of whether advisors are meeting their fiduciary duty.

Whether mandated by regulators or demanded by clients, a commitment to improving transparency in service pricing is already evident. Fee-based advisory achieves that enhanced transparency and makes client's interest the first priority, but it must be implemented on the basis of certain first principles. Private banks adopting this solution must aim to:

- Explain the all-in fee structure upfront
- Remove any commission structure that pays the advisor from product sales, e.g. removing equity trading commission, offering trailer-free funds
- Offer products without additional spreads, e.g. remove bank's FX spread, bond spread
- Absorb third-party cost (e.g. taxes, stamp duty, exchange levy) into the all-in service fee
- Eliminate any unforeseen costs.

Without the conflict of interest arising from product sales commissions, clients will perceive the all-in fee structure directly with the benefit of this advisory service model. Clients' confidence improves and banks can achieve better profit margins.

SEGMENTED PRICING STRUCTURE

Banks which currently offer fee-based advisory typically design their multi-segment pricing structures on the basis of internal cost or manpower effort. It is observed that different tiers are derived from:

- Frequency of client contact and portfolio review
- Availability of buy, sell, or switch investment ideas
- Portfolio risk monitoring and simulation
- Access to dedicated investment specialists.

Instead of product designs centred around internal profits, banks should offer this service based on client needs. In respect of those needs, banks have identified two categories of client that are attracted to this model:

- In the first category, clients do not have full faith in discretionary management. So although they do rely on investment advisors to monitor their portfolios, they still want to retain control and have the final say in every decision. They prefer a simplified fee structure, which allows them to retain the benefit of making every decision.
- The second category of clients believe they possess better investment skills than the bank, but are still willing to pay for an investment partner and to tap on the bank's research and ideas to complement their own.

When targeting a diverse range of potential clients, it is advised to highlight the different characteristics of products and services offered in each segment. To protect margins, banks are advised to run simulation models to determine the optimal all-in fee structures for each pricing segment.

GOAL-BASED PORTFOLIO CONSTRUCTION

With a fee-based subscription model relationship, clients expect a higher and more consistent quality of service offering compared to those offered on a transactional advisory basis. This enhanced quality needs to be apparent from the very beginning of investment process, namely when constructing the investment portfolio.

The prevailing offerings by private banks continue to be asset-based within the constraint of a client's overall risk tolerance and capacity. Assessing a portfolio mix typically starts with client profiling questionnaires and restrictions, asset class preferences and risk tolerance levels. The client would then select a major asset allocation from a pre-defined list of models based on various risk levels, with the ability to amend the asset class weights to a degree. The asset classes would then be broken down to sub-sector classes or to economic regions prior to clients selecting individual assets. This asset-only approach ignores the liabilities in the client's life balance sheet.

Clients tend to have many goals across their lifetime, and each has its own time horizon and risk tolerance. For instance, a medium-term goal of funding children's college education in seven years' time will have very different characteristics from a retirement portfolio that will be accessed twenty to thirty years hence. These life-event goals form the implied liabilities within the life balance sheet of a client. Given the time horizon and various risk and return expectations, each goal should be served with a separate portfolio. Hence, wealth advisors need to identify the client's preferences for risk and return for each particular goal, rather than use their overall risk profile.

For a fee-based advisory solution to serve the client's actual needs, the portfolio construction process should integrate the implied liability at inception. Only after the goal-specific risk constraints and return expectations are clearly articulated should the process continue on to asset class and asset product discussions.

PERIODIC MONITORING AND REVIEW

Many fee-based advisory solutions offer periodic portfolio reviews. These differ across competitors in terms of the frequency of monitoring materials sent to the client, the breadth and quality of portfolio indicators covered in the review material, and the frequency of direct client contact with advisors. Accordingly, clients within different pricing tiers may be offered a review quarterly or semi-annually; may have access to static portfolio health indicators or dynamic scenario and sensitivity-based stress testing; and may have scheduled monthly or quarterly advisor contact or in some cases be offered that facility on request.

For fee-based advisory to be an effective offering, it is recommended that advisors utilize the monitoring and review to support the client's ongoing relationship with the bank, identify any new implied client liabilities due to changing needs, and enforce the service-oriented relationship (rather than commission-based product sales model).

LEVERAGE ON DIGITAL CHANNEL

There is no question that fee-based advisory solutions must leverage the digital channel in serving client needs in our connected world. Some banks provide dedicated digital channels for clients of fee-based advisory, while others leverage their existing digital banking platform. Technology capabilities may differ among banks, but any strategy involving digital channels and direct human interaction needs to be clear cut from the outset, so that those channels effectively complement each other rather than confuse clients. For those banks that are still behind on the technology curve, their priority should be to eradicate the teething issues, focus the improvement on client experience, and ensure the efficiency of information delivery to the clients.

In the lifecycle of advisory communications, information delivery to clients is part of the one-way communication, and may cover:

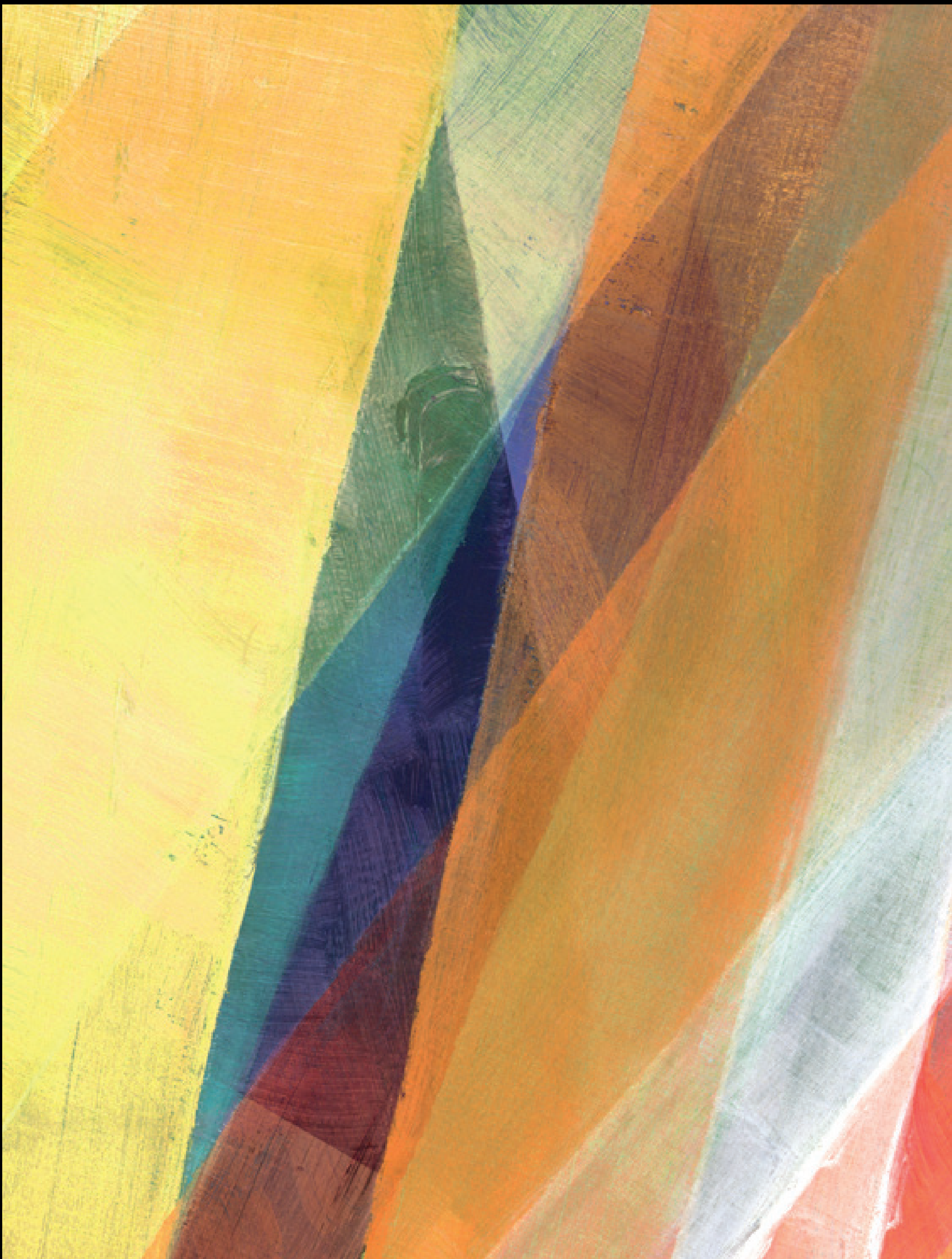
- Client statement and letters
- Trade confirmation notes and advices
- Investment proposals and product idea offerings
- Voluntary corporate action selection
- Portfolio monitoring and periodic health-check reports.

These services should leverage an efficient digital platform, enabling the client to receive and act on the information without the need to contact the advisors. For example, when an urgent risk breach occurs in the portfolio, the digital platform alerts the client and suggests options, which the client can directly execute without additional human interaction.

Advisory services should increase the digital footprint by simplifying, standardizing and publishing their services to digital channel. This frees up the two-way communication between client and advisor to focus on issues when emotional or judgemental decisions play a key role. Depending on the pricing segments and the needs of the client, either a single advisor contact or an additional investment specialist channel can be the point of contact.

CONCLUSION

Fee-based advisory will get the vote of some private banking clients. In order to distinguish itself from the competition, offering a service with transparent all-in fee structures is the right place to start. Segmented pricing tiers and a goal-oriented investment process are both key to developing scale and quality. In the digital economy, having an efficient digital channel has become essential to complement the established advisor-client relationship.



AMLD5 AND THE ART MARKET: ART MARKET PARTICIPANTS MUST NOW ACT LIKE FINANCIAL INSTITUTIONS TO MITIGATE RISKS

AUTHORS:
Jeroen Dossche, Belgium
Anthony Verhelpen, Belgium

From verifying client identity to reporting suspicious activity, art market participants have seen significant changes to the way they operate as the EU tightens regulations to combat money laundering. In this article, we look at the impact on the art market and what participants need to prioritize to ensure compliance.

Introducing several changes and new rules, the Fifth EU Directive on anti-money laundering and counter-terrorist financing (AMLD5) was adopted by the EU Commission on 30 May 2018 and should have been transposed into national law by member states in January 2020.

Although it may have been overlooked in some quarters, the obliged entities within the Directive's scope now include art market participants (AMPs). Mandatory AMLD5 compliance is a profound change that will significantly impact customer experience in the art sector, which has a long tradition of commercial and personal confidentiality.

When purchasing or selling a work of art, AMPs will now need to perform due diligence to understand who they are dealing with (customer due diligence) and where the money comes from and goes to (transaction monitoring).

It is not surprising that AMPs have been added to the list of obliged entities, considering how easily money laundering can take place in this historically opaque sector. In a recent case, a UK gallery director has been accused of accepting £6.7 million in exchange for a 1965 Picasso, Personnages. Forged ownership papers were drawn up to legitimize the sale, while keeping the Picasso stored away. The gallery director then 'pretended' to buy it back at a lower price, keeping between 5 and 10 percent of the laundered money in the transaction.[1] Similar transactions have allowed money launderers to use the art market in the past. To mitigate money laundering risks, AMPs must now start acting like financial institutions.

AMPs tried to resist their inclusion as obliged entities under AMLD5, although the impact of this change is yet to become clear. In the early 2010s, a Mexican law (similar to the EU Directives) intended to expose drug cartels and introduced client identification requirements alongside limits on prices for art-related transactions. It resulted in a 70 percent drop in sales within a year, likely because cartels were the biggest buyers.[2] Such an impact is not foreseen on the European market but art collectors, in general, are known to place great emphasis on privacy. Sharing personal information may prove an unwelcome hurdle for some of them, which could impact not only European AMPs but also the global art market.

WHO IS AFFECTED BY THE DIRECTIVE?

AMPs are defined in AMLD5 as firms or sole practitioners who are "trading or acting as intermediaries in the trade of works of art, including when this is carried out by art galleries and auction houses, where the value of the transaction or a series of linked transactions amounts to €10,000 or more" as well as "persons storing, trading or acting as intermediaries in the trade of works of art when this is carried out by free ports, where the value of the transaction or a series of linked transactions amounts to €10,000 or more"[3].

Auction houses, galleries, art dealers, advisors, free-ports, art fairs, and any other intermediaries involved in an art transaction fall within the scope of AMLD5.

AMPs are, however, exempt from such obligations if the total value of a transaction or a series of linked transactions (including taxes, commission, and ancillary costs) falls below €10,000. One might wonder about the volume of transactions that will fall in the scope of AMLD5. Even though few artists ever reach the one million US dollar level, the global average auction lot price reached $24,000 in 2019, with more than 550,000 transactions and a total turnover of $13.3 billion.[4] This only represents the tip of the iceberg, as the value of the global art market in its entirety was estimated to have reached $64.1 billion that same year. It is, therefore, safe to assume that tens, if not hundreds, of thousands of transactions will fall under AMLD5 on an annual basis.

WHAT ARE THE REQUIREMENTS IMPOSED BY AMLD5?

Regardless of the size of the business, each AMP needs to implement a robust compliance framework, which must be appropriate for addressing the money laundering risks to which the business may be exposed. This principle of the risk-based approach lies at the core of any robust anti-money laundering framework.

Understanding the specific nature of these money laundering risks requires an overall risk assessment. These risks will be different for each business. For example, a French online art gallery selling the work of young artists for €1,000 on average, with occasional bigger pieces exceeding €10,000, will have a different risk profile to an auction house operating in Paris with an average sales price of above €100,000 and an international base of customers. Both will therefore have different internal controls.

Once the risks have been identified, a framework will generally include customer due diligence and transaction monitoring measures. The framework must be documented (e.g. policies, procedures, controls) and well-embedded within the entire organization (through training, awareness, etc). AMPs are also required to appoint a dedicated anti-money laundering compliance officer (AMLCO), and records of customer due diligence must be kept securely and remain available for scrutiny.

Finally, suspicious activity reports (SARs) must be sent to competent authorities when suspicious transactions are detected. For example, a client residing in Spain wishes to purchase an artwork from a local gallery, but uses funds from an account located in the Bahamas or immediately proposes to sell back the purchased piece at a lower price. These unusual behaviors must be identified by the AMP as part of their standard transaction monitoring and may result in a SAR.

There is a lot at stake for AMPs who lack solid compliance frameworks. Failing to implement appropriate controls and recordkeeping, may result in administrative fines of up to 10 percent of the previous year's turnover – or even criminal charges. However, in a market where reputation is key, reputational damage can have a more severe impact.

IMPACT ON THE CUSTOMER JOURNEY

The pressure to perform customer due diligence prior to the delivery of the artwork could jeopardize the customer journey and relationship. Indeed, AMLD5 requires the AMP to perform due diligence on the customer, the legal representative, and the ultimate beneficiary owner (UBO) for transactions of €10,000 or more.

The parties qualifying for due diligence will differ depending on each deal set-up. For example:

- An auction house is required to perform customer due diligence on both the buyer and the seller, as they both qualify as its customers
- In the case of a private deal, where a gallery or an art dealer sells an artwork to a buyer, the customer due diligence should be performed on the buyer only.

If that same gallery or dealer sells an artwork to a buyer on behalf of a seller, the customer due diligence must also include the seller.

Due diligence typically consists of verifying the identity of all parties concerned. When dealing with an individual, valid identification documents (passport, identity cards, etc.) are required to confirm the name, family name, date and place of birth and, if possible, their address. Similar corporate documentation (bylaws, trade registry, etc.) must be obtained when dealing with a legal entity to validate the corporate name, registered office, members of the board of directors, and the ownership and control structure. The checks must be performed following a risk-based approach, allowing for simplified due diligence on low-risk clients while requiring enhanced due diligence on high-risk clients.

AMPs must also perform checks on the source of funds and the nature of the transaction or business relationship. Specific measures must be taken where certain elements of high risk are detected, such as links to a high-risk country, tax havens, or politically exposed persons.

Complexity may arise in situations involving intermediaries. Most high-value transactions involve numerous intermediaries, especially when dealing with legal entities (trusts, museums, foundations, etc.), located in different parts of the world.

For example, a seller based in France hires an agent located in the UK to sell a Concetto Spaziale by Lucio Fontana at $550,000. There is a lot of liquidity in the market for this type of work, which could make it a target for money launderers. On the other side of the transaction, the buyer located in Italy uses the services of another agent, also located in Italy. That same agent is in contact with a third UK-based agent. The two UK-based agents then conduct the transaction on behalf of the ultimate buyer and seller. In this set-up, due diligence may need to be performed by three different agents on five different participants – a total of 10 different due diligence procedures[5].

As complex as it may seem, these types of multilayered arrangements happen quite often with high-value transactions. This example also highlights the global impact of the Directive: the buyer and his agent would also be subject to customer due diligence if they are not be based in the EU, since the seller and his agent are EU-based AMPs.

CAPCO'S PROPOSED APPROACH

The complexity of AMLD5 requirements will clearly put pressure on the art sector. As stated above, AMPs are used to doing business without much scrutiny of compliance measures. Implementing an anti-money laundering framework can be challenging for international structures established within and outside the EU. Smaller businesses with no prior legal and compliance capabilities may – whether inadvertently or deliberately – fail to implement an AML framework, whether through a lack of awareness of AMLD5's importance and the potential sanctions they could face or due to the costs and complexity involved.

Building on existing capabilities and experience can help mitigate some of the challenges. Here are the four key areas to focus on to ensure successful compliance with AMLD5 requirements:

1. **Keep your customer journey at the heart of your approach:** The information required under AMLD5 will lengthen sales processes and impact your client relationships. The increase in personal information disclosure will also impact customer experiences. Keep it simple: ensure that you design a framework that can be executed while focusing on the customer journey. Being compliant with the General Data Protection Rule (GDPR), building seamless due diligence processes and transparent communication channels can safeguard client relationships and differentiate you from the competition.

2. **Safeguard your reputation:** Your reputation is built on trust from your clients. Art Tech firms offer tools to keep your client database secure, up to date and readily accessible, with a thorough monitoring process for both authentication and AML purposes. Should you identify a suspicious transaction, the availability of up to date client information and records will help you stop such a transaction while also allowing meaningful cooperation with relevant authorities. Remember the regulator's starting point: "What is not documented, does not exist". Your reputation is at stake, so do not make the mistake of underestimating the importance of a solid AML framework.

3. **Do not reinvent the wheel:** Repeating the process of providing personal information for different transactions and AMPs is tiresome and could discourage some collectors from trading actively. Establishing a central and secure registry of clients for AMPs could minimize the need for repeated individual disclosures of personal data; however it should be noted that collectors are not likely to welcome the idea of their identity being stored and shared among AMPs. You can use your existing client registry to get an overview of all the information already collected, keeping in mind that the information stored should be limited to what is necessary from an AMLD5 customer due diligence perspective, to remain GDPR compliant. This will allow you to identify gaps, avoid unnecessary workload, preserve client relationships, and align your AMLD5 and GDPR frameworks.[6]

4. **Focus on your high risks:** A granular overall risk assessment will allow you to identify risks more precisely and prevent suspicious transactions. Allocate your valuable compliance resources to high risks rather than false positives.

REFERENCES

[1] Financial Times, "Can the art world clean up its act? ", 2020, https://www.ft.com/content/a5beb8e2-5334-11ea-90ad-25e377c0ee1f

[2] Washington Post, "Mexican art galleries suffer as drug money laws end anonymous cash buys", 2014, https://www.washingtonpost.com/world/mexican-art-galleries-suffer-as-drug-money-laws-end-anonymous-cash-buys/2014/09/16/4e5dc6c4-3d41-11e4-a430-b82a3e67b762_story.html

[3] Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018

[4] Art Price, The Art Market in 2019, 2019, https://www.artprice.com/artprice-reports/the-art-market-in-2019/global-assessment-strong-and-flexible-demand/

[5] The seller's agent must conduct a due diligence on the seller (his client), on the buyer (UBO) and the agent of the buyer as well as on the intermediary agent. The buyer's agent must conduct a Customer Due Diligence on the buyer (his client), on the intermediary agent, and on the seller's agent. Note that the buyer and his agent have no obligation nor right to know the identity of the seller. The intermediary agent must conduct a Customer Due Diligence on both the buyer's and the seller's agents, as well as on the buyer (UBO).

[6] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance)

WHY ORGANIZATIONS MUST PRIORITIZE EMPLOYEE EXPERIENCE

AUTHOR:
Aditi Shukla, Germany

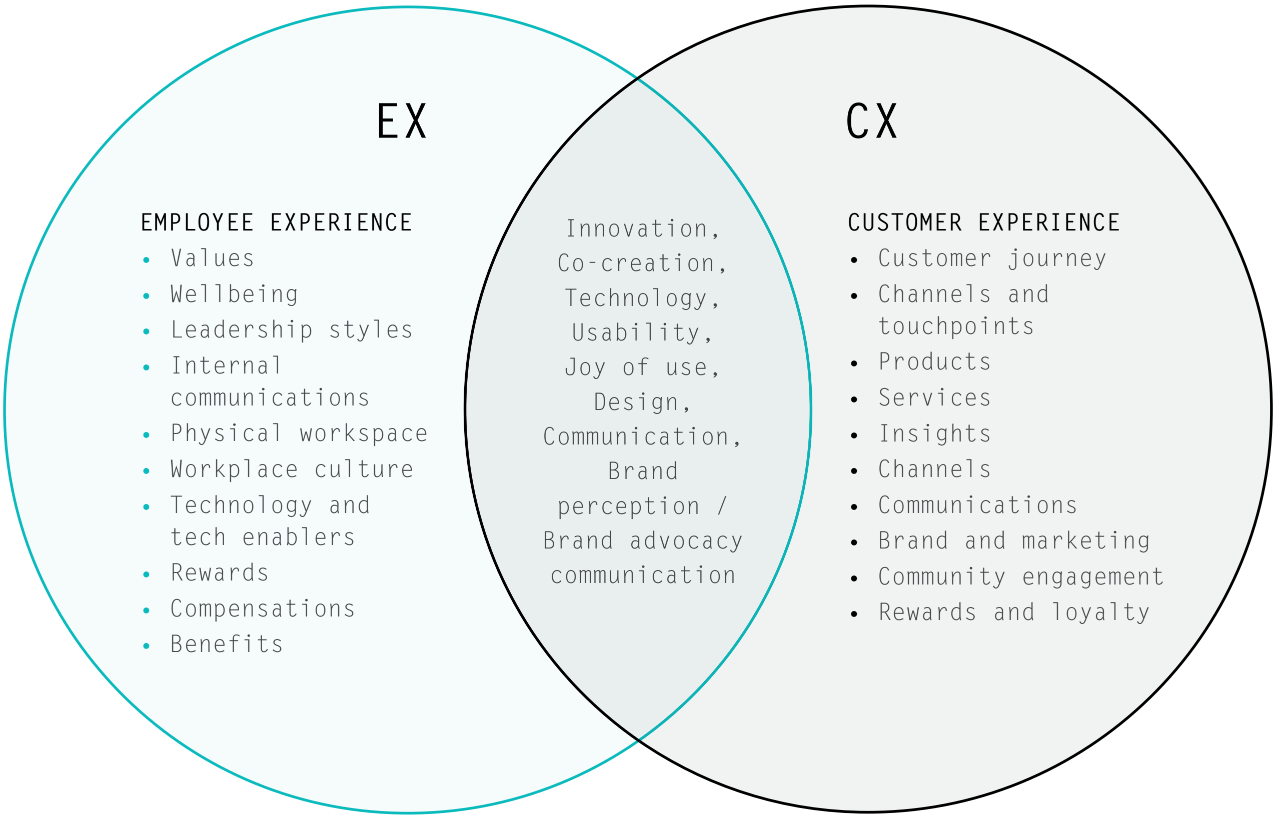
Today's global financial institutions face numerous challenges in addressing the evolving needs and heightened expectations of a demanding customer base. This generates an impetus to keep up with the latest technological advances, while also complying with increasingly complex regulatory requirements, juggling issues with legacy systems and balancing costs.

Time and again, our clients ask us to help drive internal efficiencies cost-consciously and – ever more frequently now – to strengthen the experiences offered to their end-customers, via targeted User Experience (UX) enhancements or overarching customer experience (CX) efforts.

In the chart on the next page, bank Customer Experience (CX) is the holistic sum of how customers engage with their respective banks, and is determined simply by how customers perceive their interactions with them. Rightfully, banks are now more conscious of brand perception and how it propagates amongst current and potential customers. Perception can be fickle and is influenced in numerous ways that are difficult to manage, as many personal considerations are in play: emotional, physical, and cultural.

However, there is an immense opportunity to positively influence that perception which many banks are overlooking – and it resides within their own ranks. You know about CX, you've heard about UX, now meet EX, otherwise known as employee experience.

"Employees want purposeful, meaningful work, and they want to contribute to a larger vision and mission-driven business that values, inspires, empowers and enables them."


EX
CX
EMPLOYEE EXPERIENCE
• Values
• Wellbeing
• Leadership styles
• Internal communications
• Physical workspace
• Workplace culture
• Technology and tech enablers
• Rewards
• Compensations
• Benefits
Innovation, Co-creation, Technology, Usability, Joy of use, Design, Communication, Brand perception / Brand advocacy communication
CUSTOMER EXPERIENCE
• Customer journey
• Channels and touchpoints
• Products
• Services
• Insights
• Channels
• Communications
• Brand and marketing
• Community engagement
• Rewards and loyalty

WHAT YOU NEED TO KNOW ABOUT EMPLOYEE EXPERIENCE

Employee experience encapsulates how employees engage with their organizations. This includes every single touchpoint with their company right across their employee lifecycle, and the perceptions and feelings that result.

Employee experience includes everything from interactions with recruiting teams, managers and leadership through to customer service, client onboarding, KYC, and the trade reconciliation and reporting software with which a firm empowers (or burdens) its employees. Individuals reportedly spend about a third[1] of their lives at work. Just as banking consumers seek financial products that reflect their needs and inter-connected lifestyles, so bank employees desire positive, fulfilling work experiences that reflect their personalities and lives. Or, at the very least, they don't want added frustrations as they try to complete daily tasks.

Your people are your first and greatest advocates… until they're not. Then they're your most powerful detractors and can be profoundly harmful to your brand. But let's set aside the brand benefits, though there are plenty. An outstanding employee experience maximizes internal performance by increasing overall productivity. Consider yourself – are you more productive when you're happy and empowered at work?

The research is conclusive, ample and clear: enhancing employee experience boosts business.[2]

A Gallup study found that companies which put their employees first are 21 percent more profitable, experience a 20 percent increase in sales, a 10 percent increase in customer satisfaction ratings and outperform on the S&P 500 by 122 percent.[3]

Slowly but surely, the idea that employees are expendable, just another number, is being banished from workplaces. Employees want purposeful, meaningful work, and they want to contribute to a larger vision and mission-driven business that values, inspires, empowers and enables them.

WHAT YOU NEED TO KNOW ABOUT DIGITAL EMPLOYEE EXPERIENCE

There are three major considerations when talking about EX:

1. **Physical:** Physical considerations relate to the actual workspace, the building, the desk/cubicle location, the office furniture. It even goes as far as the temperature (too hot or too cold will be distracting), how much exposure to natural light employees benefit from during the workday, the paint color of walls, the hand soap in the bathroom, or whether free fruit and coffee are provided.

2. **Cultural:** Cultural considerations include anything that affects the senses and leave an impression on employees. This is more about the attitudes of the employer and employees, the overall feeling and mindsets – it's the office buzz. For example, it could be anywhere from positive, flat and friendly to negative, hierarchical and toxic. Organizational culture is defined by the leadership team: their tone, style, and whether they exhibit the values the company publically espouses.

3. **Technological:** This is about the tools and tech resources organizations equip their people with to complete their day-to-day work, such as desktops, laptops, phones, as well as software, applications, systems (CRM, learning management, timesheets, and expense management etc.), the video conferencing setup in conference rooms, and more.

> *"WHY am I STILL manually sourcing, enriching and comparing trade data – I know this is a task which can be automated so I can focus my energy on identifying and investigating exceptions."*

WHAT YOU NEED TO KNOW ABOUT DIGITAL EMPLOYEE EXPERIENCE CONTINUED

Organizations have the power to directly influence the physical, cultural and technological factors which form the holistic employee experience. In this paper, we will focus on the technological component, and specifically the digital employee experience (DEX) – the sum of an employee's digital interactions in the workplace and their feelings, opinions or impressions of them.

Do the speech bubbles above sound familiar to you? Such scenarios are prime examples of poor DEX. Is it therefore any wonder that how people feel about their work will greatly affect their engagement and productivity? Do not undervalue emotion!

Inadequate, outdated tools that are no longer industry standard make people feel frustrated (and that their skills are out of date) which carries over into feelings about their workplace and career prospects. So, if you're still expecting your people to work with unsupported tech, like Windows Vista[4], then you better be prepared for them to say "hasta la vista… baby".

Take the time to understand the core of what your employees need to accomplish their everyday tasks. Generally, it's time (e.g. being undisturbed by superfluous meetings, IM notifications, and allowing your people the space to reach a flow state), on-demand access to information, and solid collaboration tools – technological policies or tools which inhibit this negatively impact an employee's experience.

> *"Ay yai yai, all this back and forth with the customer during the KYC process is clearly annoying to both of us – where's e-signature and 'instant KYC' when we need it!"*

THE POWER OF DIGITAL EMPLOYEE EXPERIENCE

So, what are the benefits of digital employee experience, you might ask. We believe that solid DEX investments will address workflow effectiveness (so employees find what they need and when they need it) and minimize inefficiencies (helping them find things quickly, rather than wasting valuable time on the search process). Effectively communicate and coordinate tasks, and reduce time spent in meetings for meetings' sake. Audit your tech set-up to ensure you're providing up-to-date tools, technologies and workflow systems which empower and support your employees. In turn you'll benefit from cost savings, a rise in employee engagement, productivity gains, and increased customer experience.[5]

Empowering your employees and fueling their productivity through effective DEX tools and tech is good business; and when introduced properly, will be embraced with immediate positive benefits for employees and employers alike.

HAPPIER, MORE ENGAGED EMPLOYEES

A positive DEX via frictionless digital workflow tools and superior systems demonstrates to employees that their organization wants to support them and help them succeed – resulting in more engaged, effective, and efficient employees. Happier, more engaged employees might sound like a soft benefit, but particularly in times of an increasing war for talent, their pursuit is highly relevant and therefore more strategic than you might initially think.

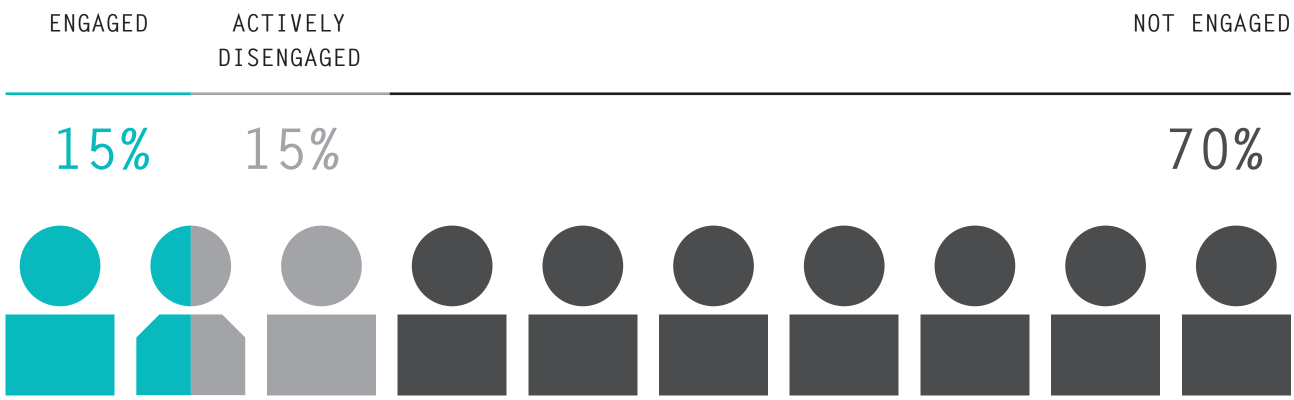
Since 2000, Gallup, an analytics and advisory company and leader in employee engagement research, has been measuring just that; and the results show that the cost of disengagement due to lost productivity are a cause for concern. The employee disengagement numbers in Germany are alarming. Gallup's State of the Global Workplace report[6] states:

- 70 percent of employees are 'not engaged', i.e. "psychologically unattached to their work and company. Because their engagement needs are not being fully met, they're putting time – but not energy or passion – into their work."

- 15 percent are 'actively disengaged', i.e. not "just unhappy at work – they are resentful that their needs aren't being met and are acting out their unhappiness. Every day, these workers potentially undermine what their engaged coworkers accomplish."

- 15 percent of German workers are 'engaged', i.e. "highly involved in and enthusiastic about their work and workplace. They are psychological 'owners,' drive performance and innovation, and move the organization forward."

The 'engaged' numbers are similar in Austria and Switzerland: 12 percent and 13 percent, respectively. So why does this matter?



THE POWER OF DIGITAL EMPLOYEE EXPERIENCE CONTINUED

The report additionally estimates an annual hit of between 80.3 and 105.1 billion euros to the German economy due to lost productivity. Further, the report cites that German companies are great at satisfying employees with vacation and job security (which it should be noted are state-mandated) but not so great at engaging them – indeed, they're "lousy at fulfilling emotional needs, such as letting people do what they do best every day."[7]

Now let's consider those percentages again and now think about the finding that engaged employees return 120 percent of their salary in value and actively disengaged employees return half that, 60 percent.[8]

Engaged employees bring more value to their organizations. People don't feed engaged if they're consistently frustrated with the tools and tech they have to use in the work place. Effective DEX helps you enable your people so they can more efficiently do what they do best and are quite literally paid to do – their jobs.

COST SAVINGS

Simply put, investing in digital employee experience improvements lead to cost savings by addressing technological inefficiencies, reducing time spent to complete tasks (i.e. reducing manual repetitive work), helping people access the information they need quicker, and increasing retention rates through increased employee engagement.

Cost savings from retention is a highly-undervalued metric. The estimated total cost of turnover ranges from values in the range of 30 percent[9] up to hundreds of percent of an employee's salary in case of client-facing or business-development roles[10]. Not least to mention it can take months to replace a skilled knowledge worker and feasibly just as long for a new hire to become up-to-speed (and able to match the productivity of the person they replaced).

Then there's the cost of overburdening the team of the leaver, as they need to cover their tasks in the interim period before their replacement is onboarded. The cost of this process is no small sum across a large institution like a bank, and it multiplies quickly in times of paradigm changes, like fintechs outmatching banks in the race for graduate talent. Alarmingly, over 63 percent of companies say retaining employees is harder than hiring them.[11]

Gallup's State of the Global Workplace report finds: "In organizations with high employee turnover, highly engaged business units achieve 24 percent lower turnover. In those with low employee turnover, the gains are even more dramatic: Highly engaged business units achieve 59 percent lower turnover. High-turnover organizations are those with more than 40 percent annualized turnover, and low-turnover organizations are those with 40 percent or lower annualized turnover."[12]

There is plenty of evidence that focusing on user experience yields quantifiable returns; and this is also true when the UX lens is internal to an organization and harnessed for EX. A cost benefit ratio of $1:$100 has been proven as a result of increasing usability across organizations. Let's take the example of a well-known computer company which simply spent $20,700 to enhance a sign-on process used regularly by thousands of their employees. This company could measure cost savings of $41,700 the very first day the new process was released. On a system used by over 100,000 people, for a usability outlay of $68,000, the same company recognized a benefit of $6,800,000 within the first year of the system's implementation.[13] Indeed, this high of an ROI is nothing to sneeze at.

ADDRESSED SECURITY CONCERNS

A strong DEX strategy can help ease the constant barrage of emails to employees and help them prioritize their work and focus their attention. In many organizations, employees are distracted by an overwhelming volume of emails, requests, notifications and reminders. This distraction diminishes engagement with the actual content of each of those emails – just because there are too many of them. This in turn can lead to spoofing and phishing scams being inadvertently replied to or acted upon without noticing.

According to European Union Agency for Network and Information Security's statistic[14], susceptibility to phishing campaigns is still high, at around 10 percent. This number has been on the decline due to awareness-raising activities, but distracted attention would likely increase susceptibility again. DEX measures can help address the security issues which arise from the many emails employees need to sift through.

THE POWER OF DIGITAL EMPLOYEE EXPERIENCE CONTINUED

ENHANCED OVERALL BUSINESS PERFORMANCE

When employees are properly equipped with the technological tools and resources they need to flourish in their roles and accomplish their daily tasks, they are more productive which in turn drives business performance.

A paper issued by research house Forrester, The ROI of EX[15], outlines the benefits of investing in EX. These include improved retention rates, increased employee referrals, reduced employee on-boarding, an uplift in profits directly resulting from employee brand advocacy, and increased productivity from improved EX.

Analytics firm Gallup has found that organizations and teams with higher employee engagement achieve the following:

Let's take the example of a piece of customer relationship management (CRM) software with a clear and intuitive UX, and that is aligned to specific departmental and organizational requirements. A top-class CRM system is a DEX tool which can help sales teams raise productivity in several ways: via effective lead management, more accurate forecasting to help meet realistic targets, by minimizing the burden of manual reporting and identifying areas for improvement.

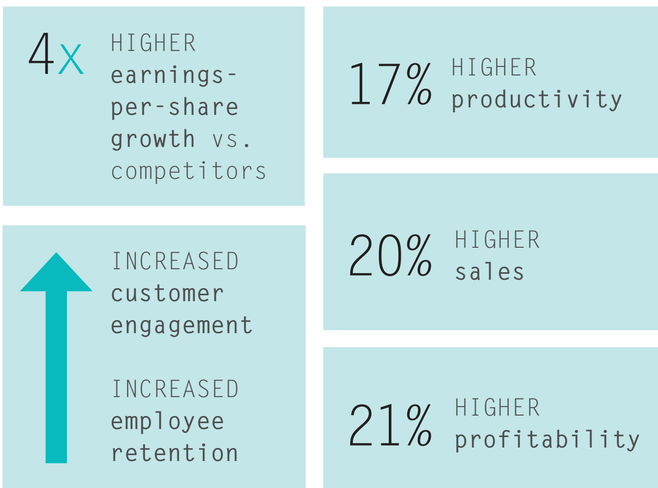
Or how about reporting? Excel is, of course, a powerful business tool that is capable of so much. Often, however, multiple spreadsheets and workbooks are utilized manually for reporting purposes; this results in additional and avoidable risk stemming from manual data entry and therefore low process efficiency.

There is very capable data visualization and reporting software available which, if implemented with strong commitment to adoption and engagement, can be highly successful in saving time and resources while also providing real-time insights to support decision making across the enterprise.

Considerable money is wasted every day because of a multiplicity or duplication of tools in combination with a lack of clear understanding as to how best to use them or transition between them effectively. Below are three examples of where we've seen this firsthand in financial services.

BANKING

While managing a global infrastructure project, this bank had to deal with a vast number of stakeholders as internal clients. The bank's CRM software, of course, was exclusively available for managing external clients and so an Excel



THE POWER OF DIGITAL EMPLOYEE EXPERIENCE CONTINUED

sheet with some 25 data columns was created and filled. Later in the project, it was determined that this database should be accessible and editable by several colleagues at the same time without creating upload conflicts.

It was therefore decided to transition the database – with hundreds of entries – into a SharePoint table. To achieve this, the project office team concluded there was no choice but to copy each Excel entry by hand into SharePoint, which took over two (well-paid) weeks. In the end it turned out, an import function was in fact available if a certain access right had been applied for by the team and would have saved much time, effort and energy if utilized to begin with. This is just one example of an efficiency that can be easily overlooked in a manual process.

INSURANCE

In terms of customer centricity and experience, the insurance industry is considered to be a leader in many ways. Nevertheless, it's not uncommon to hear that agents must juggle between 4 or 5 different front-ends when it comes to claims management, deciding on claims and coverage, and proofing for underwriting, and more.

Some insurance agents require three monitors to view all the systems they need to access regularly (consider the extra hardware cost to the organization). Imagine how often claims identifiers must be entered manually across the variety of systems in order to internally distribute claims information, to initiate payments, and so on. Consider the frustration for the agents, as well as the amount of errors and subsequent costs for the company.

Entire task forces are dedicated simply to clean up double entries. Beyond the time and money spent on reviewing this manual work, it also means disproportionate effort is expended on training agents on multiple systems and their nuances as opposed to educating them on using a concise, well-wrought integrated tool architecture. The complexity arising from the need to use a different system for each product also impairs cross-functional data collation and management, as well as employee deployment across related product lines, such as automotive and home insurance.

WEALTH & ASSET MANAGEMENT

One of Capco's international wealth management clients was using a multitude of client-serving tools and recognized it was a time-consuming task for many of their relationship managers (RMs) to analyze all client portfolios and predict next best trades. The creation of an investment proposal and simulating the impact of the recommended trades entailed multiple iterations and manual steps.

In just six weeks and employing a number of methods (contextual interviews, user journeys, design sprints, user testing, process mapping and reengineering, information architecture), we designed a DEX tool – the Portfolio Opportunity Finder – which generated user happiness scores among RMs of above 80 percent. Portfolio Opportunity Finder delivers massive time savings for RMs by automatically scanning all portfolios on a regular basis, identifying the clients who need an investment proposal, and automatically calculating fully customized 'next best move' investment opportunities.

Ultimately, good digital employee experience will positively impact an organization's bottom line. Heightened employee productivity and increased retention help an organization both make and save money.

INCREASED END-CUSTOMER EXPERIENCE

Poor EX spills over into poor CX. Actively disengaged client-facing employees will inevitably display their unhappiness via their attitude and impatience, and at some point this negativity will manifest in front of an end customer. Conversely, motivated people who take pride in their work radiate an aura of happiness and promote positive customer experiences. Organizations which are leaders in customer experience have 60 percent more engaged employees. CX-led organizations live and breathe user-centricity and recognize that their employees are essentially internal clients, leading to positive results.[16]

THE CHALLENGES

Digital employee experience has a lot of benefits but, like any change, there are quite a few organizational hurdles to overcome on the DEX track.

COMPETING BUSINESS PRIORITIES

Employee Experience is still an emerging topic. CMS Wire reports that 67 percent of organizations look at competing priorities as the biggest roadblock to EX initiatives[17]. Unfortunately, we have heard decision-makers make comments such as "Sure, we could improve this, but why would we? Our employees have to use it anyway." Such attitudes lead to a deprioritization of the Digital EX tools that are the foundation to enabling your people and propelling your business in the future.

Since there isn't yet a comprehensive understanding of the benefits of DEX or how best to measure it, it's not considered as important as, for instance, addressing regulatory topics. This is understandable as regulatory compliance is indubitably a vital priority in the here and now and failure to comply may lead to your company having no future at all. However, without proper DEX investment the future your business has may lack a competitive advantage. Investing in DEX sets your organization up for sustainable innovation and equips your people and organization for what's to come.

Promoting a clearer understanding of the straight line that connects employee experience with increased engagement and productivity is key to overcoming roadblocks. As always, money talks – providing ways to quantify savings and gains will pave the way to 'win the war' when prioritizing competing projects. Leading global banks that are increasingly 'employee-obsessed', prioritizing EX investments, are the ones with a clear competitive advantage.

RESISTANCE FROM SECURITY AND COMPLIANCE

Security and compliance get a pretty bad rap as perennial blockers of innovation due to fears of risk and vulnerability. Digital employee experience initiatives seek to innovate how we assess and equip the people who are the backbones of any business but who may initially be blocked. Resistance from security and compliance teams are consistently cited as a barrier to EX initiatives, and easing access to information and resources will help people meet their daily work goals. When employees request more up-to-date software or hardware, they're often frustrated by rigid policies that make it harder for employees to do the work their organization needs them to do.

While it's easy to blame or hide behind security and compliance considerations, it's more important for organizational leaders to work closely with those teams to find new solutions, update policies and ensure compliance with DEX initiatives. This will ensure that the twin goals of enhancing employees' overall technological experiences and boosting their productivity and engagement are not compromised.

In addition, ensuring GDPR compliance is vital for organizations, and securing your employees' data will help you form more trusting relationships with them. An active and transparent solution for employees to manage their personal data, and for how the company can use their data, will be beneficial. However, the way that compliance departments interpret the regulation can have a direct negative impact on the employee experience, particularly when it comes to the use of communication and collaboration tools. Restrictive interpretations can limit employees' ability to effectively and efficiently communicate within and across teams.

INSUFFICIENT SENIOR-MANAGEMENT OWNERSHIP

The fact that this is a topic that needs to be pushed and validated within organizations via multiple business cases means many firms aren't living the values they espouse and/or are neglectful of any considerations beyond short-term financial impacts. Caring about your employees must go beyond mere lip service and should be backed up with solid investments in tech infrastructure and policies which set your people up for success.

LACK OF A CLEAR DEX STRATEGY

Sixty percent of organizations don't see DEX as business critical, according to a survey conducted by Step Two[18], a digital workplace and intranet consultancy. As a result, they don't devote the time and effort to mapping out a unique digital experience strategy that is tied to their overall business vision and goals. This leads to many DEX initiatives lacking clear objectives, direction and metrics and to poor outputs in terms of productivity or engagement rates.

THE CHALLENGES CONTINUED

MISSING HUMAN CENTRICITY

Keeping the human at the center of employee experience is a key to building effective DEX tools. It's about designing experiences and introducing technologies which make people's lives easier by breaking down tech barriers to productivity, bolstering their efforts and providing opportunities for growth. It is not about supplanting people.

INEFFECTIVE CHANGE MANAGEMENT

Certainly, you can roll out a whole range of new and complex technologies. However, if you don't involve your people in the selection and/or build of that tech, and then sufficiently prepare them for the upcoming change via effective training programs, then they are likely to resist, or worse, fear it – thus defeating the purpose of such digital transformation.

So, where do we start?

DEX BEST PRACTICE

It takes more than ad-hoc measures to drive a strong digital employee experience. Here are some best practices we recommend:

1. ENSURE DEX IS BEING DRIVEN FROM THE RIGHT PLACE

The first step is to make the digital employee experience a priority across the whole organization.

Often any topic or issue containing the word 'employee' is pushed across to Human Resources and addressed via surveys and focused campaigns with a view to attracting, retaining and training talent. All of which is needed of course – but it does fall short, as the technological component is often overlooked or out of scope. Successful employee experience transformations are led by the C-suite, who have the authority and means to enhance technological resources and policies.

To drive DEX from the right place, a shift in perspective is generally required. Thinking of your employees as your internal clients is a helpful way to start. This is especially relevant for retail banking, where your employees may well also be actual end-customers of your bank. Even if they're not, the tone and mood they project as they talk about you or discuss their work with their friends, family and others will influence how others see your organization.

A CIO-led, cross-functional workplace experience task force, dedicated to fostering a positive workplace culture across the enterprise, would be most effective in ensuring the needs of all employees are understood and considered.

It's important to note that new tools and technology bring with them challenges in respect of engagement, adoption and training. While DEX tech promises enhanced efficiencies, engagement and progress, it also means some people may feel left behind. You must bring them along on the journey, and that starts with respecting and addressing their reservations. Successful change and training programs must have strong, transparent and honest leadership support. Be sure to prioritize this and ensure your change drivers are effectively empowered.

DEX BEST PRACTICE CONTINUED

2. FORM A CLEAR DEX STRATEGY BASED ON EMPLOYEE NEEDS

Is it any great surprise that when employees talk about their employers on social media, the most common emotions are negative rather than positive?[19]

Regardless of your opinion of social media channels and their users' motivations, it's clear that there is an abiding sense across social posts that employee needs are not being respected. It is worth noting that female-identifying social media users are more vocal about their jobs online than their male-identifying counterparts.[20]

Being empathetic and getting to know your people is fundamental, be it their needs, motivations or painpoints. Simply introducing customer experience methods within the firm isn't enough. CX initiatives are meant to satisfy and engage customers who interact with banks maybe a dozen times a year. Rebranding and rolling out those same initiatives internally will fall short when it comes to employees who spend so much of their lives working for you.

Consider how the cultural and technology environments you provide to employees helps them directly in achieving their everyday work goals – and also where they fall short.

Moreover, don't presume to know what your employees feel – you must ask them. If you doubt they will be 100 percent honest in their responses, then create a mechanism for them to feedback anonymously via a survey tool or alternatively by nominating one person in each team to collect their colleagues unidentified responses.

Survey questions to employees could include:

- Which technology tools provide the most value for you during the working day?

- a) What is the tool, or aspect of a tool, that we use that most impedes your job?

  b) How much time do you typically lose struggling with this tool each day?

- Are there tools that you have used in your previous employment(s) that would help you do your current job more effectively?

- Are there any tools that you use at work which you require more training on? (please specify which tool and in which areas you require reskilling or a refresh)

- How can we improve your digital employee experience?

Insights formed during this process will not only help your business become more attuned to your employees' needs, but will also create a clearer vision and strategy for the future.

3. FOCUS ON MAPPING EMPLOYEE JOURNEYS

Something wonderful happens when you help your employees succeed in their day-to-day lives and defeat cumbersome systematic barricades that are outside their control. Simply put, they thrive – and so does your business. Achieving this outcome requires both an understanding of their daily lives and the sort of robust, informed insights which are derived from scrutiny of individual's interactions with the technology ecosystem.

If something is difficult to do, or requires extra effort, we're likely to put it off. Accordingly, find out which technologies are getting in the way, and why. Investigate how many 'clicks' it takes to complete certain tasks and in particular examine any process required to complete those tasks with high abandonment rates. Establish feedback loops, and (anonymously) ask your employees which tasks they particularly hate.

Doing so will typically unearth a plethora of workflow weaknesses and inefficiencies. Again, as per the previous step, it is essential that your employees are truly involved in the diagnostic process. Don't just map what you think someone's journey is – involve them to ensure you're accurately capturing their everyday experience.

Also, invest in DEX across the board. Your employee journeys shouldn't merely comprise those individuals sitting in head office. Your branch employees are just as important – if not more so – to your organization and the nurturing of your brand. It's

GLOBAL ONLINE CONVERSATION SAMPLE			
POSITIVE POSTS ABOUT WORK, JOBS AND EMPLOYERS	NEUTRAL POSTS ABOUT WORK, JOBS & EMPLOYERS	NEGATIVE POSTS ABOUT WORK, JOBS AND EMPLOYERS	TOTAL NUMBER OF POSTS ABOUT WORK, JOBS AND EMPLOYERS
1,104,578 **(16%)**	2,051,950 **(30%)**	3,691,712 **(54%)**	6,848,240

Brandwatch search, February 2019 to February 2020.

GLOBAL ONLINE CONVERSATION SAMPLE DURING PEAK-LOCKDOWN PERIOD			
POSITIVE POSTS ABOUT WORK, JOBS AND EMPLOYERS	NEUTRAL POSTS ABOUT WORK, JOBS & EMPLOYERS	NEGATIVE POSTS ABOUT WORK, JOBS AND EMPLOYERS	TOTAL NUMBER OF POSTS ABOUT WORK, JOBS AND EMPLOYERS
293,330 **(15%)**	438,162 **(22%)**	1,264,154 **(63%)**	1,995,646

Capco search using Brandwatch for the period of 1 March 2020 to 6 May 2020

TOP THREE EMPLOYEE GRIPES PRIOR TO THE WESTERN CORONAVIRUS LOCKDOWNS
• Low pay
• Bad management
• Long work hours

Capco search using Brandwatch for the period of February 2019 to February 2020

TOP THREE EMPLOYEE GRIPES DURING PEAK LOCKDOWN PERIOD
• Poor communication from management
• Low pay
• High expectations

Capco search using Brandwatch for the period of 1 March to 5 May 2020

DEX BEST PRACTICE CONTINUED

especially important to identify and to smooth out customer-facing employees' technological painpoints, as they have a direct influence on the end-customer experience.

4. SELL DEX

Selling the digital employee experience journey is essential. Swiftly rolling out a great suite of technological tools and resources is all well and good – but if not embraced by your people, your mission will inevitably fail. Your best bet for success lies in a strategic approach to change management, fueled by education and communication that drives behavioral change, increases knowledge, and fosters engagement and adoption via authentic, accessible and value-aligned delivery.

We recommend you employ effective communications and change-management campaigns, and ensure transparency throughout the entire journey. Be honest about your goals around technological empowerment – and that to enable your people, you need their help to succeed.

It is extremely important never to hide obstacles and problems employees are likely to encounter en route to success. Don't pretend their day-to-day won't change – but if DEX initiatives are successful, those changes will be for the better. Nevertheless, it is still change and will require all the effort that any change entails. To that end, be prepared to answer the all-important question – "what's in it for me?" – at every stage of the journey, and for every department or individual in scope.

5. WEAVE A UNIFIED DEX

At one time of another, many of us will have had to manually enter the same data into multiple systems. We know how annoying it is. This is expected when individual business units develop or procure different technologies and independently set up processes and governance mechanisms tailored to their own specific requirements. Duplicative pathways are created when system updates and evolutions are implemented differently across siloed organizations. Consequently, from approval and transaction requests through to receiving services, employees end up having to interact with multiple points of contact.

Think back to when you've been a new joiner at a company. Onboarding is so rarely seamless: many parts of the process are disjointed and require the employee to provide the same background or security information to different parts of the company repeatedly – whether simply to get a laptop working, their salary or benefits paid, or even to get security access to open a door. It's no wonder that a mere 12 percent of employees highly rate their company's onboarding process.[21]

Integrating all business platforms and apps within a clean, branded front-end will create a seamless digital experience for your internal users. A unified, user-friendly digital employee experience platform will ensure a 'one-stop-shop' for your employees, while a consolidated management dashboard will help monitor this.

6. FACTOR IN REMOTE READINESS

As stated at the outset, our technology expectations have been heightened by the world around us. Right now, that world is in the midst of the COVID-19 pandemic. During these times, we're especially reliant on accessible and reliable technology to keep us connected with our co-workers and loved ones alike (not to mention our reliance on life-saving medical technology).

Amongst other things, the coronavirus crisis has demonstrated that many workers can effectively operate remotely. A March study by Glassdoor found that three out of five US employees are confident in this way of working.[22]

Let's also not forget that many employees want to work remotely. An IBM study of 25,000 adults in May 2020 found that 54 percent would like to work primarily from home once offices reopen.[23] Moreover, a Leadership IQ study conducted before the coronavirus crisis found that remote employees are 87 percent more likely to love their jobs compared to those working in offices[24].

Prior to the pandemic, Capco published a paper – The Workforce of the Future A New Hope[25] – which found that adopting flexible working patterns improves a firm's productivity, profits and reputation. As employees and employers alike come to recognize just how much can be done from home, and as work-life balance continues to come to the fore, there will likely be a greater push for true flexibility in the workplace.

Some academics believe COVID-19 will accelerate the fourth industrial revolution and digitalization of all services, including

DEX BEST PRACTICE CONTINUED

public services[26]. Certainly, an organization that builds an effective remote digital workplace will be better positioned to innovate, drive productivity and collaboration, and attract the employees it needs to remain competitive in any sort of future remote working-oriented situation.

7. INSTITUTE VALUE METRICS AND CONTINUOUS IMPROVEMENT

The ability to harness and visualize data to form 'actionable' insights is critical in the growth journey of all organizations. Building in ways to measure the impact of new systems/tools/technologies is key. Initially, this can help showcase the value derived from DEX investments, but beyond that it can also help you scale or optimize your business for the future.

Being able to see where and how efficiencies were – or were not – achieved along enhanced employee journeys will help inform you on how next to proceed. By tying DEX success metrics to overall business performance metrics, you can see the emergence of a more positive income-to-cost ratio, customer-satisfaction metrics, and employee-engagement data, for example. This can help you make the case for continued DEX and EX investments, which will only add to your competitive advantage in the marketplace, both amongst your end-clients and your internal ones.

CONCLUSION

Your employees define and embody your brand – and their performance, productivity and engagement will shape your future. Accordingly, EX – and DEX – should inform all your strategic decision-making.

As COVID-19 in particular has demonstrated, understanding the human needs of colleagues is essential for successful cooperation – and not just in the customer experience arena – and will promote a healthy nurturing workforce culture.

If you're in the financial services industry, we encourage you to reflect on the digital employee experiences you've have had in the past and to challenge the status quo by:

- **Strengthening the user experience you provide for internal applications** – this is foundational in providing a solid employee experience, driving productivity, engagement and fueling competitive advantage;
- **Identifying, improving/building, managing and continuously measuring** specific elements or segments of your customer or employees experience to increase revenues or create efficiencies, including any software implementation;
- **Leveraging design methodologies** to enhance or otherwise boost a current proposition, or to rapidly prototype from scratch and determine which ideas to take forward from idea to MVP
- **Driving engagement and adoption around change** (technology, process, regulatory, cultural/workforce) by properly preparing your people and organization for the changes associated with the introduction of new technologies into your workforce;
- **Enhancing employee experience via effective learning and communications** that drive behavior change, increase knowledge, and drive engagement and adoption via authentic, accessible and value-aligned delivery. The benefits will filter though into the customer experience.

REFERENCES

1 https://www.gettysburg.edu/news/stories?id=79db7b34-630c-4f49-ad32-4ab9ea48e72b&pageTitle=1%2F3+of+your+life+is+spent+at+work

2 https://services.forrester.com/playbook/The+Employee+Experience+Playbook+For+2020/-/E-PLA500

3 https://news.gallup.com/reports/191489/q12-meta-analysis-report-2016.aspx

4 https://support.microsoft.com/en-gb/help/22882/windows-vista-end-of-support

5 https://www.forrester.com/report/The+ROI+Of+EX/-/E-RES145895

6 https://www.gallup.com/workplace/238079/state-global-workplace-2017.aspx

7 https://www.gallup.com/workplace/238079/state-global-workplace-2017.aspx

8 http://info.frontstream.com/rs/frontstreampayments/images/EmployeeEngagementeBook.pdf?mkt_tok=3RkMMJWWfF9wsRonuavLZKXonjHpfsX57+gsWKaxlMI/0ER3fOvrPUfGjI4ATsZkI+SLDwEYGJlv6SgFQrPHMbds0bgKWRc=

9 https://www.benefitnews.com/news/avoidable-turnover-costing-employers-big?

10 https://retensa.com/clients/clients-by-industry/banking-finance-turnover/

11 https://blog.smarp.com/employee-engagement-8-statistics-you-need-to-know

12 https://www.gallup.com/workplace/238079/state-global-workplace-2017.aspx

13 Usability: A Business Case, Human Factors International, 2005.

14 "ENISA Threat Landscape Report 2018"

15 https://www.forrester.com/report/The+ROI+Of+EX/-/E-RES145895

16 Forbes: The Un-Ignorable Link Between Employee Experience and Customer Experience, Forbes, 23 February 2018.

17 Digital Employee Experience Still Not Viewed as Business Critical, CMS Wire, 27 March 2019.

18 Elevating the Employee Experience in a Digital-First World, Whatfix.com, 3 October 2019.

19 Analysis of social media mentions for February 2019 to February 2020 and March - May 2020 respectively by Capco using Brandwatch, which captured a sample (50 percent) of online mentions on employee gripes to provide an accurate value of the social media conversation.

20 Analysis by Capco using Brandwatch for February 2019 to February 2020, and 1 March - 6 May 2020 found that 54 percent of the conversation around employer issues was by female-identifying users.

21 Employee Experience surveys, Gallup.

22 New Survey: COVID-19 & Employee Sentiment on Changing Workforce, Glassdoor, 23 March 2020.

23 54 Percent of Americans Want to Work Remote Regularly After Coronavirus Pandemic Ends, New Poll Shows, Newsweek.com, 4 May 2020.

24 You're 87% More Likely to Love Your Job If You Work from Home, LeadershipIQ.com.

25 The Workforce of the Future: A New Hope, Capco, December 2019.

26 Our Lives After the Coronavirus Pandemic, AlJazeera.com, 26 March 2020.

WHY ARE SO FEW FINANCIAL SERVICES FIRMS REALIZING TANGIBLE BENEFITS FROM MACHINE LEARNING?

AUTHOR:
Edward Pease, UK

Machine learning (ML) has well and truly entered the dictionary of oft-used corporate buzzwords in the last few years. You only need to look at the increase in the number of Google searches (see below) to see a steady increase in interest over the last decade.

INTEREST IN MACHINE LEARNING OVER TIME

Figure 1. Interest over time in the term 'machine learning'. The number of searches is scaled to a number between 0 and 100 so 100 represents peak interest

Source: Google Trends

So what actually is machine learning? Think of it as Software 2.0.[1] In traditional software (Software 1.0), rules are hardcoded such that specific inputs lead to defined outcomes. For example, if a customer alerts a company that they want to move to a competitor, some software could send them an email offering a 10 percent discount for the rest of the year. For machine learning (Software 2.0), the rules are not explicitly defined but are learnt using data. In our previous example, using historical data about which customers have left the company and which have not, an algorithm could be learnt to predict which customers are most likely to leave. It might be that low account usage is a particularly predictive factor. The marketing team could then use this information to decide to send them a discount voucher proactively rather than reactively. As it turns out, this use case, namely 'churn prediction,' is a common ML use case.

It is certainly true that technology companies have led the way in using ML to improve customer experience and increase revenue. Amazon[2] uses powerful forecasting algorithms to predict demand for product lines ahead of time. Netflix's recommendation algorithm has been so successful that the company revealed that 80 percent of content is watched based on the algorithm's suggestions.[3]

Google, as you would imagine, makes extensive use of ML but in my mind one of the most striking is their subsidiary DeepMind using ML to reduce the cooling bill for their datacenters by a staggering 40 percent.[4]

However, in financial services (FS), ML is still a largely untapped opportunity. If you search for 'machine learning case studies in financial services,' you get a lot of results about how transformative ML could be and very few tangible results along the lines of, 'We implemented ML for this use case and saved $[x]m'. Sure, not every financial institution will choose to publicly talk about this, but the lack of concrete examples is particularly striking, particularly given the published use cases available in other industries. During this piece, we simply ask 'why is this the case'?

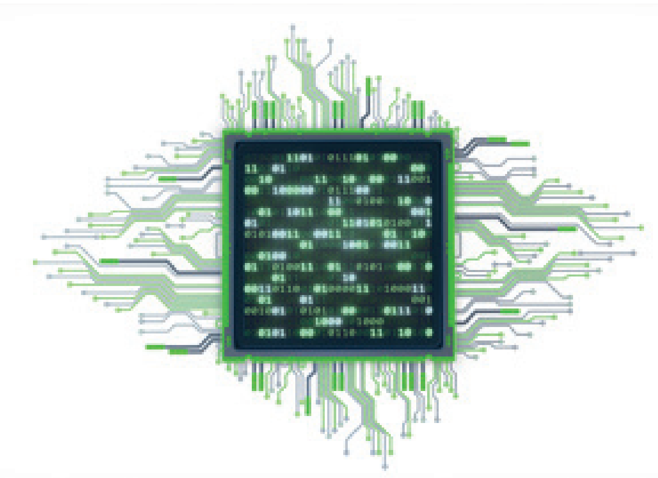
> “*It will empower every business, every government organization, every philanthropy. Basically, there's no institution in the world that cannot be improved with machine learning.*”
>
> Jeff Bezos, Amazon CEO

THE BARRIERS TO MACHINE LEARNING ADOPTION

There are certainly lots of reasons as to why implementing ML in a corporate setting is not easy. Gartner[5] have done some extensive research (in all industries, not just financial services) on the state of artificial intelligence (AI) adoption and the most frequent barriers preventing AI adoption:

These survey results are a great overview of the different reasons as to why ML adoption in the enterprise is not easy. ML is not unusual in that respect – history shows us that transformative technologies often take time to be fully adopted in an enterprise setting. In Capco's experience for financial services specifically, the main barrier to ML adoption in our industry is a cultural one: getting ML practitioners (often called data scientists) and management to understand each other better.

Figure 2. The most frequently cited barriers to AI adoption



A FEW CAVEATS…

Machine learning doesn't work for all use cases and certainly isn't the nirvana that it is sometimes portrayed. If your data is patchy, badly structured and/or siloed, then a data cleaning or data rationalization project might well need to take place in parallel alongside your ML proof-of-concept. ML as a technology has similarities to the relational database innovations of the 1980s – both technologies are of limited use without data!

A good rule of thumb is that the more consequential each individual decision, the more cautious you should be about ML. If the Spotify recommendation algorithm plays a song I don't like, it is not a big issue and I spend little time pondering why it chose this track before hitting the skip button. However, if a ML algorithm tells me that I have cancer after analyzing a scan, I will want to know how and why it came to that conclusion.

But there are lots of use cases in financial services where ML can be used appropriately and could make a huge difference. From our extensive experience in working with financial services firms, we think the following shifts in mindset are required.

FOR DATA SCIENTISTS…

When deciding whether to go ahead with a ML project, realize that your management will not necessarily be interested in ML per say, but interested in *whether it can solve their business problems*. This is a crucial distinction – people who have the internal resources to commit to ML projects are not likely to be as impressed as you are in the latest deep learning algorithm.

When the project has started, it is always important to aim for a least a few quick wins to help build trust. Although tackling the problem properly may take a couple of months, some meaningful insights along the way can help bring people along with you. Also, make sure that you always keep in mind the materiality of what you are working on. It might take a couple of weeks to increase the accuracy of a model from about 73 percent to 80 percent. But the real question is: to what extent would business outcomes improve with this increase in accuracy? If the effect is negligible, then time is probably best spent elsewhere. On the subject of which, it is also important to appreciate that, depending on the use case, understanding why a model has made a prediction is often as important as the model accuracy.

At the end of a project that has got great feedback, bear in mind that it will probably still take a while to get your model into production and so to have a large business impact. Even if your ML approach for a particular problem is vastly superior to an existing process, do not underestimate the time it will take for people to change from a process that they are already familiar with. This time will also likely shorten as ML adoption increases in your organization.

FOR DECISION MAKERS…

ML will be able to have a large impact in your organization so fully leveraging this technology will put you at an advantage against your competitors. When beginning your ML journey, it is always best to start small, then test and iterate from there. An iterative approach will enable you to become more comfortable with ML and therefore feel more able to factor ML results into your decision-making process. So, rather than relying on just intuition and retrospective analysis, you can also take account of predicted future outcomes too.

Now, it is certainly possible to do this while appropriately managing the risk – it is imperative to start small before scaling. This iterative and agile approach will also help to get key internal stakeholders to trust ML decisions.

The benefits of machine learning are not a future hypothetical; they are happening now. A few use cases that have been implemented in financial services firms are:

- **Capacity modeling** – building a 'capacity calculator' to enable efficient resourcing in back-office functions
- **Reducing manual reviews** – automating the review of legal documentation[6]
- **KYC optimization** – predicting file completion times to identify bottlenecks in the KYC process
- **Predicting client profitability** – using ML to predict the profitability of clients, helping relationship manager to prioritize their time and unprofitable clients to be flagged.

HOW CAN FIRMS OVERCOME THESE CHALLENGES?

While the challenges of realizing significant value from ML might be daunting, it is more than possible. Capco's top three tips for ML success are:

1. Having a laser-like focus on solving high-value business problems, rather than simply doing interesting experiments or analysis

2. Starting small, testing and working in an agile manner to quickly uncover what is possible

3. Having a plan to implement successful work into internal dashboards and processes to maximize impact and awareness across the firm

CONCLUSION

Machine learning is a transformative technology which, when used well, can help to reduce costs, increase revenue, and provide better customer experience. Fully realizing the benefits of machine learning certainly isn't easy but it is probably easier than you think to get started. To make the most of machine learning, a cultural shift is needed from both data scientists and decision makers.

REFERENCES

[1] https://medium.com/@karpathy/software-2-0-a64152b37c35

[2] https://forecasters.org/wp-content/uploads/gravity_forms/7-c6dd08fee7f0065037affb5b74fec20a/2017/07/Januschowski_Tim_ISF2017.pdf

[3] https://www.wired.co.uk/article/how-do-netflixs-algorithms-work-machine-learning-helps-to-predict-what-viewers-will-like

[4] https://deepmind.com/blog/article/deepmind-ai-reduces-google-data-centre-cooling-bill-40

[5] https://www.gartner.com/smarterwithgartner/3-barriers-to-ai-adoption/

[6] https://digital.hbs.edu/platform-rctom/submission/jp-morgan-coin-a-banks-side-project-spells-disruption-for-the-legal-industry/

CYBER HYGIENE: HOW TO DISINFECT DIGITAL PAYMENTS AGAINST FRAUD

AUTHORS:
Julien Bonnay, US
Bryce VanDiver, US

For all the devastation that COVID-19 has wreaked worldwide, one impact has escaped widespread notice. COVID-19 accelerates payments attacks against financial institutions, consumers, and even companies as the pandemic changes buying habits and promotes a shift to remote work.

The pandemic has motivated consumers to rely more on contactless digital payments over cash as a hygiene measure. This contributed to a 32 percent increase in digital payments[1] at the start of the pandemic, although somewhat mitigated since the economy soured.

Another way to look at the payments shift is through the eyes of cybercriminals, who see a veritable greenfield in fraud opportunities, today and increasingly in the future as digital payment options proliferate. In April, Financial institutions (FIs) reported a 35 percent jump in dollar volume[2] of attempted fraudulent transactions year over year, according to Fidelity National Information Services Inc., known as FIS. And the head of cybersecurity for VMware told a House subcommittee[3] in May that cyberattacks against the financial sector rose by 238 percent between February and April, just as COVID-19 was gaining strength. The increasing use of remote workers only offers more exposure to employers struggling to update cybersecurity measures.

But COVID-19 is increasing a trend that was already prevalent. Over the last few years, several trends have converged to make cyberfraud more of a threat to institutions than ever. For one, fraudsters have become bigger, bolder, and more sophisticated – even several nation-states appear to be backing attacks on ATMs, FI databases, and skimming payment cards during brash point of sale attacks.

The story isn't just about bigger and better criminals, however. If Willie Sutton robbed banks because "that's where the money is," today, the money is everywhere: in transactions bouncing off of satellites, initiated on mobile phones, streaming through undersea cables, and in personal financial data stored on servers. According to the GSMA Mobile Economy Report 2018, 71 percent of the world's population could have access to digital payment technology[4].

The corporate shift to the cloud has opened an entirely new arena for hackers to play in, with massive breaches exposing tens of millions of accounts. And the tools of the trade cybercriminals use are better, too. An eye-opening spoof attack[5] in the United Kingdom in 2019 used artificial intelligence (AI) and technology-enabled voice mimicry to convince a company employee to wire $243,000 into the account of thieves. The loss was relatively small potatoes among cyber exploits but a gigantic warning that fraudsters are once again upping their game and challenging the FI to respond.

Is there a path towards disinfecting digital payments despite current trends and the arrival of even more threats? We believe there is. By strengthening security around digital payments, hardening defenses in the cloud, and encouraging consumer-education campaigns, we see the foundation of cyber hygiene steps for building a resilient payments future.

WHERE ARE THE NEW THREATS COMING FROM?

Digital technology has created incredible opportunities for banks and other FIs to explore new business strategies and market opportunities. But digital technology also has armed criminals with new tools, such as AI and machine learning (ML), to create data breaches, trick consumers, and worm into what companies believed were secure data centers and payment processing programs.

To be sure, cybercrime was already on the rise over the past few years. One measure of increasing criminal activity has surfaced in cybersecurity breach disclosures. According to Audit Analytics (Trends in Cybersecurity Breach Disclosures, May 2020), there has been a 54 percent increase in breaches since 2017[6], a rogues' gallery of crimes including malware attacks, phishing, spoofing, and exploiting IT misconfiguration vulnerabilities. Since the start of the COVID crisis, however, it feels as if fraudsters are cashing in on the gift of chaos, and incidents will mutate even more virulently if not checked.

"We need to anticipate the specter of knowledgeable attackers gaining the sophistication to understand and deploy AI/ML capabilities, to make their attack attempts more scalable and lethal," argues Paul Rohmeyer, a financial cybersecurity expert who runs the FinCyberSec conference at the Stevens Institute of Technology. "Responding to AI/ML-driven cyber risks will create requirements for new skillsets, an understanding of how AI/ML can potentially manipulate vulnerable systems and personnel, and a focused observation on developments across the financial industry as these threats move closer to reality."

Fraud, of course, is as old as financial services themselves. What is new is who is doing the defrauding and how they are doing it. Here is a glimpse at the new landscape.

NATION-STATE-SPONSORED ATTACKS

FIs had it relatively easy when they were battling individual fraudsters and teens with too much time on their hands. Now they even have to go up against rogue state-sponsored attackers.

North Korea, in particular, is believed to target payment systems and banking to raise funds to support weapons development. The country was implicated in the theft of millions in bitcoin and 'cryptojacking' computing resources to mine bitcoin. North Korea was also suspected of stealing millions from ATMs in Asia and Africa, and possibly made off with $81 million in a fraudulent SWIFT network transaction[7]. Given global sanctions taken against the country, coupled with its weapon development aspirations, expect North Korea to continue to invest aggressively in these types of attacks. According to an advisory[8] issued by the U.S. Department of State and other federal agencies in April, North Korea's "malicious cyber activities threaten the United States and the broader international community and, in particular, pose a significant threat to the integrity and stability of the international financial system."

Other state actors suspected of supporting cybercriminal activity include Russia, Pakistan, and China. Between March 1 and March 13, 2020, for instance, the largest number of targeted spear-phishing campaigns originated in China[9], according to cybersecurity operator Intsights.

CRIME IN THE CLOUD

After a slow start in early 2010, companies moved to the cloud at an amazing clip, including payment systems and data. The cloud brings obvious benefits to FIs, such as using automation to continuously updating cyber protection software. The cloud is also an ideal location to launch AI- and machine-based learning programs to detect fraud patterns and even deploy defenses as attacks are happening.

However, the consolidation powers of the cloud also mean that minor mistakes in the configuration of one area can amplify into a catastrophic loss. Even the most sophisticated cloud defenses may not be up to the challenge to fend off a criminal who uses psychology to fool employees to hand over the keys to the gold room. Most breaches can be tracked back to human error.

CASE STUDY: CAPITAL ONE AND THE $72 MILLION MISCONFIGURATION ERROR

Capital One was considered an antifraud poster child – until it was hit in 2019 with one of the largest cybersecurity crimes on record. A 33-year-old software engineer wormed her way into credit card applications left vulnerable by a misconfigured software firewall, allowing her to access a server where the credit applications were stored. The breach affected 100 million U.S. consumers, compromised 120,000 Social Security numbers, and exposed credit monitoring, offset by $34 million in insurance recoveries.

CREDIT CARD ACCOUNTS STOLEN IN POINT-OF-SALE (POS) BREACHES

It was thought (or maybe just hoped) that prevalent use of card chips in the United States would curtail POS breaches. But security surrounding these transactions remain vulnerable to skimming and other forms of attack. Sophisticated cybercriminals have learned how to suck out the purchase data and even record PIN entry at the store counter. Another approach is for fraudsters to infect a retailer's payment system with malware, collecting transaction data. That's what happened at a breach at Saks Fifth Avenue and Lord & Taylor[10] in 2018, affecting up to 5 million customers. The criminals used a phishing expedition to gain access through an employee's computer.

Expect adversaries to continue to focus on these vulnerabilities, given the easy payoff. Credit card fraud is no small problem. As the most common type of identity theft each year, reported dollar losses in 2019 were about $135 million[11], according to the U.S. Federal Trade Commission.

Changing consumer behavior caused by the pandemic is also likely to create more opportunities for cybercrime. We believe card-not-present (CNP) breaches will jump given increases in online shopping driven by the pandemic. An AITE Group report predicts a 16.4 percent increase in U.S. CNP fraud in 2021[12].

B2B SCAMS TARGETING HIGH-VALUE TRANSACTIONS

Payment scams, of course, are hardly limited to the retail world, although retail is the primary focus here. It's worth noting that on the B2B payment front, increasingly sophisticated adversaries are going after high-value transactions such as wire transfers. In one of the more innovative attacks, pretexting was combined with AI to mimic the voice of a CEO with a slight German accent to authorize a quick wire transfer of $243,000[13] to a fraudulent location. This type of fraud will increase as adversaries hone their technical skills and add emerging technologies into their toolkits.

CASE STUDY: CHUBB LOSES $4.8 MILLION COVERAGE CLAIM IN SPOOFING ATTACK

In June 2014, an accounts payable employee at Medidata Solutions received an email purportedly from the company's president that ultimately led to her wiring $4.8 million to a fraudulent account. A subsidiary of Chubb Insurance refused to pay an insurance claim from Medidata, arguing that an attack on the insured's email system was outside coverage boundaries. The U.S. District Court in New York ruled against Chubb. "Medidata has demonstrated that its losses were a direct cause of a computer violation," the court ruled.[14]

MOBILE BANKING ATTACK

Most FIs offer mobile applications for customers to access their assets remotely. This trend has been reinforced during the pandemic when many banks shut their lobbies. According to the FBI, a 50 percent spike in the usage of banking apps has been observed since the start of 2020.[15]

"The FBI expects cyber actors to attempt to exploit new mobile banking customers using a variety of techniques, including app-based banking trojans and fake banking apps," the agency announced in June. While mobile apps might appear to be secure on the surface, they are, in truth, vulnerable because they lack critical security features. Criminals have noticed, responding with fake banking apps and banking trojans, including MazarBot, BankBot, LokiBot and Anubis.

BUSINESS PROBLEMS FOR FINANCIAL INSTITUTIONS

Fraud losses—including losses linked to credit and debit cards – cost U.S. banks, merchants and cardholders $16.9 billion in 2019, up 15 percent from a year earlier and the highest amount since 2013, according to Javelin Strategy & Research[16]. Companies reporting the highest costs related to payment card and bank account breaches since 2013 were Equifax, $1.7 billion; Home Depot, $298 million; and Target, $292 million, according to Audit Analytics.[17]

But the ramifications for businesses or institutions targeted by payments fraudsters go way beyond money loss. Here are just a few shockwaves exploding out from a breach that can cause lasting damage.

Loss of investor confidence: A high-profile hit can turn a profitable quarter into a losing year, dragging down stock prices and investor confidence with it. After Target's breach, sales dropped 4 percent and its profit plunged nearly 50 percent the following quarter[18]. The share price fell 46 percent and the CEO resigned. Conversely, when Home Depot suffered a high-profile attack in 2015, proactive action and communication by the CEO not only limited damage in the stock market, the company added 25 percent in shareholder value[19] that year.

Brand damage: A corporate brand can take decades to build, but only a few news cycles to destroy following a data attack. In the United Kingdom, a breach at telecommunications provider TalkTalk resulted in the loss of 101,000 customers[20] after their private information was compromised, and they revolted on social media. A 2019 study by Radware[21] reported that 43 percent of companies that took part in the study experienced sour customer experiences and reputation loss due to a successful cyberattack.

Recovery burden: In the 12 months following a breach, small- and medium-sized companies faced, on average, $1.2 million in compromise costs and $1.9 million in business disruption costs in 2019, according to the Ponemon Institute[22]. Some other costs are incalculable, but still injurious. Consider the overall drain on corporate resources consumed with answering jammed support lines, communicating with vendors and key stakeholders, dealing with insurance companies and regulators, and putting out fires with institutional investors.

Liability issues: Who is liable when fraudsters pull off a payments heist? Traditionally, in CP cases, the bank issuing the card took the hit but now, the burden seems to be shifting to retailers. To escape that liability, merchants must install secure systems. Still, costly POS devices like Chip-and-PIN readers – an expense that already stressed restaurants and other shop owners find it difficult to pay. This is a hotly contested development that is far from settled.

CASE STUDY: COVID-19 PANDEMIC CAUSES INCREASE IN CYBER FRAUD

Millions of consumers have shifted their banking and purchasing activity to online channels since the coronavirus outbreak forced mandatory stay-at-home orders. Employees of most major businesses are also working from home full-time during the crisis.

The changes in e-commerce and mobile banking have created entirely new targets for hackers to exploit weaknesses in remote corporate networks, merchant e-commerce sites and financial institutions dealing with massive increases in mobile banking transactions. In February 2020, Lookout Phishing AI discovered a campaign that used SMS messaging to target customers to fake websites of well-known banks in Canada and the U.S., including Scotiabank, CIBC, HSBC, Chase and others. The campaign was designed to capture the banking credentials and login information of users.[23]

EFFECTIVE STRATEGIES TO CONQUER DIGITAL PAYMENT FRAUD

As we explored, digital payments crime is increasing and increasingly sophisticated trends like work-at-home promote a shift to digital payments. The good news is that improving technology such as AI is available to help conquer digital fraud, although the fix will also require ever-increasing vigilance by FIs themselves and significant help from consumers.

Here are actionable recommendations for FIs to follow beyond increasing the basic rules of cyber hygiene, such as motivating customers to frequently change strong passwords, use two-factor authentication, and rigorous rounds of software patching and keeping on top of security updates. The recommendations can be summed up easily:

1. Use intelligence to anticipate threats and mitigate loss

2. Reduce the attack surface internally and in the cloud

3. At POS, incentivize the use of Chip and PIN readers and tokenization

4. Educate consumers

USE INTELLIGENCE TO ANTICIPATE THREATS AND MITIGATE OR LIMIT A LOSS

In erecting barriers to the most sophisticated or powerful cybercriminals, especially those related to state-sponsored actions or B2B scams, the best mitigation is usually intelligence. Knowing who your adversary is, their likely methods of attack, and their motivations serve as the base for a threat intelligence-driven strategy.

There is a robust market for cyber threat intelligence, so it is widely available to payment processors and card providers. The difficulty for the FI is not intelligence, but rather the time to analyze the data and apply it to the threats facing the individual organization. Too often, this intelligence is unused, cast off to a deep corner of a remote data warehouse.

We believe FIs would be well served to build a capability around what is commonly called a Cyber Fusion Center (CFC). The CFC is the next generation of the Security Operations Center (SOC), which organizations have depended on historically to detect attacks and contain the damage. By contrast, the CFC extends well beyond this classic “moat and castle” defense.

Think of the Cyber Fusion Center as a platform that combines functions such as Cyber Threat Intelligence, Red Teaming, and Attack Surface Reduction, and makes them highly visible throughout the organization. To do so, CFCs integrate functions such as plant security, SecOps, and IT operations to promote more effective threat intelligence, creating a more proactive, collaborative, and unified approach to negating threats.

With a clear understanding of their own strengths and weaknesses, layered with actionable intelligence, FIs should set strategic and tactical priorities based on the actions and capabilities of their adversaries, their attack surface, and with a focus on the most critical payments systems and data.

But the old wisdom still stands when it comes to the basic blocking and tackling of cybersecurity: continually update your network security systems; partner with verified payment processors; keep

CASE STUDY: COVID-19 PANDEMIC CAUSES INCREASE IN CYBER FRAUD CONTINUED

on top of crime trends; ensure that tokens and login credentials are regularly changed, ensure your protections against internal threats are strong and embrace the many other hygienic basics you should already be following.

REDUCE THE ATTACK SURFACE INTERNALLY AND IN THE CLOUD

The boom in Internet-exposed assets from years of digital transformation, and accelerated by a seismic shift to a remote workforce in response to COVID-19 can make protecting your FI's digital attack surface feel overwhelming. FIs are responsible for defending their internal network and their digital presence across the internet and the cloud.

Bringing the enormous scope of an organization's attack surface into focus helps frame the challenges of extending cybersecurity outside the corporate firewall, especially as staff forced to work from home push that boundary farther out. One way to do it, is to red team the cloud and other pathways and blind spots that hackers are exploiting.

Red teams are a favorite tool of the military, and their task is simple: find flaws in the organization that can be exploited by the enemy. Red teamers, who report to and are supported by top commanders, are granted much leeway to act like insurgents and reveal vulnerabilities invisible to the rest of the organization. We think every medium- and large-scale organization should create a red team to attack itself using a three-tiered attack-and-discovery approach of 'outsider with no knowledge,' 'outsider with limited knowledge,' and 'an insider with knowledge' to provide a real-life test of their exposure to known security vulnerabilities.

But organizations need to do more to make sure they are organizationally prepared to block cyber threats. These include:

- **Incentivization:** Successful security is as much a mindset as a battle plan. The message must be pushed down from the top and accepted as part of the corporate ethos by every employee. Incentivize your team to get it right – "what gets checked, gets done."

- **Training:** Over half of all FI breaches are due to human error, especially in areas like support or customer service, where reps are more concerned with satisfying the customer than checking for security vulnerabilities. Invest in training and build systems that are resilient to user missteps. Special focus should be placed on senior leaders to heighten awareness of emerging threats.

- **Keep your software, hardware and cloud up to date:** Many hackers make a fine living off of companies who fail to keep security patches up to date or keep too much legacy or open-source software running in vulnerable areas. While pure cloud companies are usually well prepared for security maintenance, those that use the cloud but still rely on on-premise technologies can be vulnerable.

AT THE POINT OF SALE, INCENTIVIZE THE USE OF CHIP AND PIN READERS AND TOKENIZATION

Card payment fraud at POS continues to grow despite the fact that the industry now has the tools to put a serious dent into these crimes. The problem isn't the lack of technology, but rather consumer wariness over new technology and a slow-building tension between banks and merchants over payments liability.

Credit cards are invitations to steal for one simple reason: the information needed to make a card purchase – account number, expiration date, and security number – are all on the card itself. A fourth security measure, the zip code of the cardholder, is rarely requested at POS. Fraudsters can steal card information in many ways, including phishing, stealing database records, and skimming from card readers (See case study below).

Two technologies can lead the defense at POS transactions: Chip and PIN and tokenization. Unfortunately, in the U.S., too many merchants still accept cards with user information embedded on magnetic stripes, a technology from the 1960s. As a secondary check, retailers ask for the user's signature, scrawls that are rarely challenged. These technologies and procedures subvert the benefits of enhanced security provided by Chip and PIN.

CASE STUDY: COVID-19 PANDEMIC CAUSES INCREASE IN CYBER FRAUD CONTINUED

Chip and PIN: Almost every credit card issued in the U.S. is equipped with an EMV chip, or "Europay, Mastercard, and Visa" technology, and many also carry a mag stripe as well. The cards come in two flavors: Chip-and-Signature and Chip-and-PIN. From a security standpoint, Chip-and-PIN is the gold standard and is used predominantly in Europe, where fraud rates are significantly lower than in the U.S. According to Barclays[24], the UK has seen fraudulent card transactions decline nearly 70 percent since adopting Chip and PIN cards.

However, Chip-and-Signature remains the preferred card type issued by FIs. Given the obvious security benefits, why is Chip and PIN not the standard in the U.S.? The catch for American consumers, some argue, is the inconvenience of having to remember and enter a PIN instead of just scribbling a signature. And for retailers, there can be additional costs associated with acquiring PIN devices, training staff, and educating users. For businesses like restaurants, which already operate on slim margins, the expense of installing dozens, hundreds, or even thousands of devices can be daunting.

Tokenization: Simply put, is the process of exchanging a meaningful piece of data, like an account number, with a token or useless piece of information. When a consumer presents a tokenized payment card at the point of sale, the holder's primary account number is not exposed, so a fraudster has no incentive to go after the transaction. The information obtained, a random string of characters will be meaningless.

Also, The PIN is not stored on the merchant's device, servers, or the servers controlled by the digital wallet provider. First introduced in 2001, digital tokenization is proven, secure, and trusted. Tokenization is gaining popularity, at least by some card vendors. PayPal, Venmo, Zelle, Google Pay, and Apple Card, and Amazon Pay are examples of tokenized products.

We believe the U.S. must join with Europe, Canada, and most other developed nations to make Chip and PIN the standard retail payments device at the point of sale, and to support other products that use tokenization to enhance security. Fraud activity will diminish, and users will feel more secure.

CASE STUDY: 30 MILLION WAWA CUSTOMERS BREACHED

On December 19, 2019, popular grocery chain Wawa revealed a stunning breach[25]. It announced that malware attached to payment card readers at "potentially all Wawa locations" had scraped off credit card and debit card numbers, expiration dates, and cardholder names on up to 30 million customers. The stolen data was later put up for sale on Joker's Stash , the internet's largest card fraud exchange. The company faces class-action lawsuits from consumers, financial institutions, and employees.

EDUCATE CONSUMERS

A primary goal of the financial industry is to move consumers to use more secure technology, such as mobile wallets and digital payments. Unfortunately, American consumers aren't on board. In an eye-opening Marqeta consumer survey[26], 80 percent of respondents stated, incorrectly, that a physical card is safer than a mobile wallet. At the same time, over half (54 percent) responded that the risk of fraud made them less likely to try newer payment technology.

But 77 percent of respondents did say they would choose to shop at a merchant who did not store their information in favor of one that did. Indeed, 75 percent said they would be willing to manually enter their payment information repeatedly rather than have it stored by a merchant, indicating that the extra one-time step of loading a payment card in a digital wallet would not be a hurdle if security benefits were better known. In other words, they embrace tokenization, even if they're not sure of what it is or how it works.

These attitudes mark a massive failure to educate consumers on how to make more secure payments by both the financial industry itself and technology companies who sell these products. For example, consumers worried about protecting their personal data and guard against identity theft should know that when a payment card is tokenized and inserted into a digital wallet on a mobile device like a smartphone or smartwatch, it loses its value for fraudsters.

CONCLUSION: IT'S A NEW DAY REQUIRING NEW WAYS

Digital payment systems are under attack as never before, a trend that the pandemic has only hastened as consumers change their buying behavior, and organizations face criminals with more sophisticated tools.

The sophistication of fraudsters is increasing – just look at the recent exploitation of flaws in the SS7 mobile data network that plays a critical role in directing traffic in most telecom networks. Metro Bank in the UK acknowledged in 2019 that hackers were able to exploit SS7 to track phones remotely and intercept messages to authorize payments from accounts[27]. Attacks on networks rather than on specific companies allow fraudsters to pull off massive breaches that affect millions of customers and cost companies millions in compensation, legal fees, and brand erosion.

Given these shifts in the threat landscape, it's no longer an option, if it ever was, for FIs to simply adopt a "moat and castle" defense, where the ramparts are raised in anticipation of an attack. FIs need to go on the offensive by investing in the latest technology, leveraging cloud protections, educating consumers and training their own organizations to be actively searching for threats.

"Attackers regularly recalibrate their objectives based on emerging technical vulnerability discoveries and in response to learning of successful attacks launched by others," says Paul Rohmeyer. "It is a never-ending cycle, and a sound cyber strategy must be informed by the prevailing threat and vulnerability landscape."

One door left unlocked is enough to results in millions in losses, many unhappy customers, and headlines that no CEO or investor wants to read. And even when COVID dissipates, the impetus it has given cybercriminals since 2020 will remain, perhaps to accelerate again on whatever disaster the next passing breeze brings us.

REFERENCES

[1] https://www.aciworldwide.com/news-and-events/press-releases/2020/may/nearly-half-of-consumers-are-more-concerned-about-risk-of-payments-fraud-due-to-covid-19-crisis

[2] https://www.wsj.com/articles/borrower-beware-credit-card-fraud-attempts-rise-during-the-coronavirus-crisis-11590571800

[3] https://www.atmmarketplace.com/articles/cyber-fraud-surges-as-covid-19-changes-banking-e-commerce-2/

[4] https://www.forbes.com/sites/danieldoderlein/2019/03/18/moving-towards-a-cashless-society-in-a-cash-reliant-world/#6a8cc82a236a

[5] https://www.wsj.com/articles/fraudsters-use-ai-to-mimic-ceos-voice-in-unusual-cybercrime-case-11567157402

[6] https://www.auditanalytics.com/doc/AA_Trends_in_Cybersecurity_Report_May_2020.pdf

[7] https://www.pymnts.com/news/security-and-risk/2018/bangladesh-bank-heist-swift-phishing-scam-fraud-doj/

[8] https://home.treasury.gov/policy-issues/financial-sanctions/sanctions-programs-and-country-information

[9] https://wow.intsights.com/rs/071-ZWD-900/images/Cyber%20Threat%20Impact%20of%20Covid19.pdf

[10] https://www.marketwatch.com/story/saks-lord-taylor-data-breach-may-affect-5-million-customers-2018-04-01

[11] https://www.ftc.gov/system/files/documents/reports/consumer-sentinel-network-data-book-2019/consumer_sentinel_network_data_book_2019.pdf

[12] https://www.atmmarketplace.com/blogs/the-perfect-theft-the-increase-in-card-not-present-fraud/

[13] https://www.wsj.com/articles/fraudsters-use-ai-to-mimic-ceos-voice-in-unusual-cybercrime-case-11567157402

[14] https://www.businessinsurance.com/article/20180706/NEWS06/912322505/Chubb-unit-Federal-Insurance-Co-must-cover-Medidata-spoof-email-loss-appeals-cou

[15] https://www.ic3.gov/media/2020/200610.aspx

[16] https://www.javelinstrategy.com/coverage-area/2020-identity-fraud-study-genesis-identity-fraud-crisis

[17] https://www.auditanalytics.com/doc/AA_Trends_in_Cybersecurity_Report_May_2020.pdf

[18] https://www.nbcnews.com/business/business-news/target-settles-2013-hacked-customer-data-breach-18-5-million-n764031

[19] https://www.aon.com/getmedia/2882e8b3-2aa0-4726-9efa-005af9176496/Aon-Pentland-Analytics-Reputation-Report-2018-07-18.pdf?utm_source=aoncom&utm_medium=storypage&utm_campaign=reprisk2018

[20] https://www.aon.com/getmedia/2882e8b3-2aa0-4726-9efa-005af9176496/Aon-Pentland-Analytics-Reputation-Report-2018-07-18.pdf?utm_source=aoncom&utm_medium=storypage&utm_campaign=reprisk2018

[21] https://www.radware.com/newsevents/pressreleases/2019/average-cyberattack-exceeds-1-million

[22] https://www.keepersecurity.com/ponemon2019.html

[23] https://www.atmmarketplace.com/articles/cyber-fraud-surges-as-covid-19-changes-banking-e-commerce-2/

[24] https://squareup.com/us/en/townsquare/why-is-the-u-s-the-last-market-to-adopt-chip-cards#:~:

[25] https://krebsonsecurity.com/2020/01/wawa-breach-may-have-compromised-more-than-30-million-payment-cards/

[26] https://pages.marqeta.com/hubfs/pdfs/Marqeta_2020_Fraud_Report_2020.pdf

[27] https://www.fintechfutures.com/2019/02/uks-metro-bank-hit-by-ss7-attack/

ABOUT CAPCO

Capco is a global technology and management consultancy dedicated to the financial services industry. Our professionals combine innovative thinking with unrivalled industry knowledge to offer our clients consulting expertise, complex technology and package integration, transformation delivery, and managed services, to move their organizations forward.

Through our collaborative and efficient approach, we help our clients successfully innovate, increase revenue, manage risk and regulatory change, reduce costs, and enhance controls. We specialize primarily in banking, capital markets, wealth and asset management and insurance. We also have an energy consulting practice in the US. We serve our clients from offices in leading financial centers across the Americas, Europe, and Asia Pacific.

WORLDWIDE OFFICES

Bangalore	Geneva	Paris
Bangkok	Gurgaon	Pune
Berlin	Hartford	São Paulo
Bratislava	Hong Kong	Singapore
Brussels	Houston	Toronto
Charlotte	Kuala Lumpur	Vienna
Chicago	London	Warsaw
Dallas	Mumbai	Washington, DC
Dusseldorf	Munich	Tysons Corner
Edinburgh	New York	Zurich
Frankfurt	Orlando	

CAPCO.COM

CAPCO