THE CAPCO INSTITUTE
JOURNAL
OF FINANCIAL TRANSFORMATION

ORGANIZATIONAL

How can banks empower their customers to flag potential vulnerabilities?

PRZEMEK DE SKUBA | BIANCA GABELLINI | JESSICA TAYLOR

ARTIFICIAL INTELLIGENCE

#58 NOVEMBER 2023

a wipro company

THE CAPCO INSTITUTE

JOURNAL OF FINANCIAL TRANSFORMATION

RECIPIENT OF THE APEX AWARD FOR PUBLICATION EXCELLENCE

CONTENTS

TECHNOLOGICAL

OPERATIONAL

ORGANIZATIONAL

DEAR READER,

As the financial services industry continues to embrace transformation, advanced artificial intelligence models are already being utilized to drive superior customer experience, provide high-speed data analysis that generates meaningful insights, and to improve efficiency and cost-effectiveness.

Generative AI has made a significant early impact on the financial sector, and there is much more to come. The highly regulated nature of our industry, and the importance of data management mean that the huge potential of AI must be harnessed effectively – and safely. Solutions will need to address existing pain points – from knowledge management to software development and regulatory compliance – while also ensuring institutions can experiment and learn from GenAI.

This edition of the Capco Journal of Financial Transformation examines practical applications of AI across our industry, including banking and fintechs, asset management, investment advice, credit rating, software development and financial ecosystems. Contributions to this edition come from engineers, researchers, scientists, and business executives working at the leading edge of AI, as well as the subject matter experts here at Capco, who are developing innovative AI-powered solutions for our clients.

To realize the full benefits of artificial intelligence, business leaders need to have a robust AI governance model in place, that meets the needs of their organizations while mitigating the risks of new technology to trust, accuracy, fairness, inclusivity, and intellectual property. A new generation of software developers who place AI at the heart of their approach is also emerging. Both GenAI governance and these 'Developers 3.0' are examined in this edition.

This year Capco is celebrating its 25th anniversary, and our mission remains as clear today as a quarter century ago: to simplify complexity for our clients, leveraging disruptive thinking to deliver lasting change for our clients and their customers. By showcasing the very best industry expertise, independent thinking and strategic insight, our Journal is our commitment to bold transformation and looking beyond the status quo. I hope you find the latest edition to be timely and informative.

Thank you to all our contributors and readers.

Lance Levy, **Capco CEO**

HOW CAN BANKS EMPOWER THEIR CUSTOMERS TO FLAG POTENTIAL VULNERABILITIES?

PRZEMEK DE SKUBA | Senior Consultant, Capco
BIANCA GABELLINI | Consultant, Capco
JESSICA TAYLOR | Consultant, Capco*

ABSTRACT

Customer vulnerability is one of the key concerns of the Consumer Duty regulation, a very welcome ESG-aligned enhancement of financial institutions' governance. Adherence to the regulation requires a clear focus on data collection that helps lenders manage the impact of consumer vulnerabilities without imposing penalties or resulting in a negative impact on clients. There are two parts of the problem that need to be addressed: firstly, how to capture vulnerability data by encouraging clients/consumers to voluntarily submit the information (the behavioral aspect) and secondly, how to technically capture, manage, and store this data to ensure compliance with the Consumer Duty regulation. This article considers both problems and reviews the tools from behavioral science that can encourage customer disclosure and two key technology solutions (data lakes and blockchain) to comply with the capture, management, and storage of data whilst remaining GDPR compliant and fully aligned to the objective of voluntary submission of information regarding vulnerabilities by clients/consumers.

1. INTRODUCTION

The Financial Conduct Authority (FCA) led consultations in 2021 that resulted in the development of the Consumer Principle (Principle 12), putting the onus on the U.K. organizations within its scope to "act to deliver good outcomes for retail customers" from 31 July 2023. Sheldon Mills, the Executive Director at the Consumers and Competition department of the FCA has specifically pinned this responsibility on the "boards and senior management [who] have a critical role in overseeing firms' implementation of the Duty. That is why [the FCA has] strengthened the requirements around governance and accountability to ensure senior managers and executives are held accountable."[1] This development highlights the growing importance of ESG and is a very welcome improvement in governance – the "G" in ESG.

Even though the U.K. already has some of the best governance frameworks in the world, one does not have to look far for warnings of what can happen when consumers are not properly protected. Poland – despite enjoying the status of a developed (per FTSE) economy with the fifth largest GDP in the E.U. – is a great case in point: an extreme example of an industrialized European country where a combination of very lax consumer protection and an incredibly light-touch financial market regulation has allowed for a mass proliferation of toxic financial products dressed up as foreign currency denominated mortgages. The problem has been allowed to fester for close to two decades now, with a peak in 2007 when "over half of Polish mortgages were issued in Swiss francs." It took several interventions by the European Court of Justice in the past couple of years to finally prompt the Polish courts to begin

* We would like to thank Julia Shreeve (Business Consulting sponsor), Martha Ferez (Behavioural Science Practice Lead), and Mark Profeti (Blockchain subject matter expert) for their support and advice with this article.

[1] FCA, 2022, "What firms and customers can expect from the Consumer Duty and other regulatory reforms," Financial Conduct Authority, Speech by Sheldon Mills, Executive Director, Consumers and Competition, delivered at the Consumer Protection in Financial Services Summit, https://tinyurl.com/ycyav7rc

annulling some of the Swiss-franc mortgages "after ruling that banks used "abusive" foreign exchange rates."[2] Importantly, on top of causing misery for millions, this has also resulted in a systemic risk to the Polish banking system.[3]

Fortunately, the U.K. has never had to deal with this sort of a problem, and indeed the Consumer Duty regulation goes even further in protecting consumer rights, with the policy placing the importance of customer vulnerability as its key priority. Of a particular note are the following paragraphs:

- **1.16:** which requires "firms to consider the needs, characteristics, and objectives of their customers – including those with characteristics of vulnerability – and how they behave, at every stage of the customer journey." It raises the bar with regards to consumer protection required of the regulated companies.
- **8.5:** which highlights that "many respondents queried the practical application (…) considerations relating to potential vulnerabilities; and the proposed approach to testing communications." Consequently, it highlights the interest expressed by those consulted in the practicalities of flagging up potential vulnerabilities.
- **10.6:** which presents the view of the consumer organizations that "suggested that firms should be required to take an inclusive design approach to meet the needs of customers with characteristics of vulnerability." Hence, clarifying the user requirement with regards to the functionalities for flagging potential and actual vulnerabilities.
- **Annex B 2A.7.4 G:** specifies that "in relation to the needs and characteristics of retail customers, a firm should, among other things: (…) **(4)** assist frontline staff to understand how to actively identify information that could indicate vulnerability and, where relevant, seek information from retail customers with characteristics of vulnerability that will allow staff to respond to their needs;" – thereby clarifying the requirement for the vulnerability flagging functionality from the point of view of the financial institutions, as well as "**(5)** set up systems and processes in a way that supports and enables retail customers with characteristics of vulnerability to disclose their needs."[4]
  – Hence providing a further clarification on the user requirement with respect to the same functionality.

As such, the FCA makes the requirements regarding any processes pertaining to the flagging of potential and actual vulnerabilities clear, with only two key outstanding questions remaining: how to encourage consumers to voluntarily submit their vulnerability data and which technology would best suit this use case.

2. THE PROBLEM

While the Consumer Duty regulation is clearly a step in the right direction as far as governance is concerned, the main problem that needs to be addressed is that customer vulnerability is a dynamic concept (i.e., it changes over time), and currently financial institutions take a static approach. More importantly, financial institutions have no proper mechanisms for monitoring customer vulnerabilities. As an example, mortgage customers will only have the KYC (know your customer) due diligence at the point of applying for the product, and even then, the KYC will not necessarily capture any vulnerabilities, as it is designed with AML (anti-money laundering) in mind. The lender will typically only find out about any vulnerabilities their customer may have been suffering from when they go into arrears with their mortgage. This is a common theme across the financial services industry, not just within home financing or general lending.

The other issue is the desire to protect one's privacy, or sometimes even the shame of admitting a problem or a weakness, as well as the natural human propensity to protect one's interests by presenting oneself as stronger, and more in control than one may be. Going deeper into human psychology to assess why customers may be opting not to disclose, behavioral science would classify these fears as "inherent biases".

2.1 Behavioral biases

Firstly, there are biases that cause people to omit negative information, such as "omission bias".[5] The "omission bias" describes how voluntary oversights are empowered by our inner belief that, ceteris paribus, committing an action is more

[2] Minder, R., 2022, "The mortgage time bomb ticking beneath Poland's banks," Financial Times, November 13, https://tinyurl.com/4s5ffzp4
[3] de Skuba Skwirczynski, P., 2021, "Swiss franc mortgages: European banks are profiteering from the Polish subprime loan plight," The Quarterly Journal of the International Union for Housing Finance, Summer, 28-32, https://tinyurl.com/bdds9vfw
[4] FCA, 2022, "A new Consumer Duty," Feedback to CP21/36 and final rules, Policy Statement PS22/9, July, Financial Conduct Authority, https://tinyurl.com/yw6mm3p
[5] Caviola, L., A. Mannino, J. Savulescu, and N. Faulmüller, 2014, "Cognitive biases can affect moral intuitions about cognitive enhancement," Frontiers in Systems Neuroscience 8, https://tinyurl.com/593pvu3d

dangerous than omitting an action. On this basis, disclosing something is perceived as a favorable action to take and customers prefer to assume the risk of hiding important information. As it is well publicized, repayment history is one of main factors affecting credit score.[6] As such, even though flagging a vulnerability does not imply arrears, it may nevertheless be cognitively associated by a customer with presenting themselves as being at an increased risk. Flagging up any vulnerability may be associated in a similar fashion with making one look riskier to the lender, and by extension to the credit scoring company, which could in turn be mistakenly perceived as negatively affecting the availability of future financial products.

Secondly, there are biases that blind people from negative information, pushing them towards an overly optimistic evaluation. Behavioral scientists call this "optimism bias" and some of its implications are people underestimating the risk of having low savings, aging, or their caring responsibilities. In these cases, omission does not spring from a forward looking and well-thought strategy, but from a purely involuntary reflex; a constructed belief in a positive outcome in which the customer is the first to believe in. In view of all this, we understand that disclosure action implies a great challenge, particularly when lenders rely on customers to take the initiative to indicate actual and potential vulnerabilities.

With that in mind, not only are customers likely to withhold their vulnerabilities but they are also less likely to disclose certain vulnerabilities than others. Considering self-disclosure types per the various vulnerabilities, as defined by the FCA (Table 1), some, such as visual impairments and poor English language skills, are more likely to be self-disclosed than others, such as mental health conditions and an income shock. That would be not only due to a perceived associated stigma, the unwillingness to admit "failure", but also for the (more practical) fear of being "blacklisted" from future financial products or having the existing mortgage revoked, however unfounded these assumptions may be. Considering the latter examples, the challenge for lenders is to create an atmosphere where customers believe they can safely share information pertaining to such vulnerabilities by way of self-disclosures.

3. THE SOLUTION

A tough question to answer is whether it is even feasible to create an environment where customers would take it upon themselves to flag up their observed or potential vulnerabilities. This question boils down to assessing what the possible resulting benefits or incentives for the customer could be.

3.1 How to capture vulnerability data by encouraging clients/consumers to voluntarily submit the information

Addressing "inherent biases" is key to considering any potential solutions for self-disclosing of potential vulnerabilities. The solution must significantly contribute to creating an environment where customers feel encouraged to disclose potential vulnerability-driven cashflow problems before they occur. This precarious stage is sometimes referred to as "pre-arrears", and some examples could include employees anticipating a redundancy, the self-employed observing worsening market conditions and consequently the

Table 1: FCA-defined self disclosure types[7]

HEALTH	LIFE EVENTS	RESILIENCE	CAPABILITY
• Physical disability • Severe or long-term illness • Hearing or visual impairment • Mental health condition • Addiction • Low mental capacity or cognitive disability • Being "older, old" i.e., >80 • Being young • Non-standard requirements or credit history	• Retirement • Bereavement • Income shock • Relationship breakdown • Domestic abuse • Caring responsibilities • Other, i.e., leaving care, migration or seeking asylum, human trafficking or modern slavery, convictions	• Inadequate (outgoings exceed income) or erratic income • Over-indebtedness • Low savings • Low emotional resilience	• Low knowledge or confidence in managing finances • Poor literacy or numeracy skills • Poor English language skills • Poor or non-existent digital skills • Learning difficulties • No or low access to help or support

[6] https://tinyurl.com/4hh67v9w
[7] https://tinyurl.com/45wp6u2k

likelihood of work drying up, or one's mental or general health worsening, all of which could ultimately lead to the borrower going into arrears.

To the lender, customer vulnerability is either disclosed by the person in question or inferred about them, with a clear preference for the former because the lender, just as much as anyone else, prefers to be certain of the risks, as opposed to having to infer them.

Consequently, to approach this from the customer's perspective, the main question is about what the lender, as the party to the contract who commands more power, should be doing to increase their customers' willingness to disclose any anticipated cashflow problems. Currently, the customer has little insight into the data held on them by the financial institutions and ancillary enterprises, such as credit scoring companies. Of course, GDPR has given customers the power to demand the data held about them from any such institutions, but these rights hardly mean that such data would be available at the touch of a button. In practice, extracting it could be a lengthy and painful process, with the necessity to write Freedom of Information requests and waiting for weeks at a time for a response. Banks could help by creating an environment where customers would be more willing to disclose their vulnerabilities by increasing transparency surrounding personal data gathered and building trust with their customers.

Another positive for the customer resulting from self-disclosure could be staying in control of exposing one's vulnerabilities. Having a say in the timing and manner of such a disclosure would grant the customer the power to control the narrative of their vulnerabilities, thereby ensuring they can present it in the best possible light. That would not be possible in a situation where the lender finds out about the issue via a third party, for example, once the customer is already in arrears. Such an approach is akin to a "controlled fall" technique taught to frail patients and high-performing sportspeople to help them prevent unnecessary injuries. Overseeing exposing their own vulnerabilities to others could be particularly attractive to customers who appreciate being in control.

Behavioral science could be applied to identify appropriate techniques that lenders could apply to encourage their customers to self-disclose vulnerabilities as opposed to having them inferred. In the context of the Consumer Duty, some of the applicable strategies that can be adopted by financial institutions are "nudges", which encourage better decisions by making certain choices easier than others, and "sludges", which discourage decisions by making the process more difficult.

Examples of nudges include:

- **Precommitment:** asking the borrower to confirm at the beginning of every fiscal year that the information held by the lender is still relevant and that they commit to notify the lender in case of any changes. Studies have shown that this technique is effective, as it facilitates the retrieval of intentions in our memory and reduces the probability of past actions impacting future behavior.[8]
- **Social norming:** emphasizing what most people are doing while promoting the correct behavior can influence borrowers' behavior, as it provides social rules and standards to follow.[9] Captions such as "nine out of ten customers have reviewed their parameters this year" leverage our inner need to feel included in a wider group (known as the "the bandwagon effect" and "herd mentality").
- **Default rules:** presenting a list of opted-in conditions from which the consumer is asked to opt out when these do not apply reduces the friction of telling the truth that is "already being told" in the presented conditions, in which case there is no further action for the customer to take. On the contrary, lying would mean actively removing the tick when asked to opt in.[10]
- **Disclosure:** disclosing the cost of the customers' omission, either by sharing the economic loss of misinformation or the financial penalty for providing inaccurate information, will make the consumer completely aware of the granular and wider consequences of their actions, thereby putting in doubt the safety of their passivity.
- **Graphic warnings:** leveraging the use of large or bold fonts attracts borrowers' attention in support of the promoted behavior as well as to support knowledge of misinformation risks (i.e., "omission effect"). This approach is commonly used with respect to cigarettes and tobacco products, and it has so far proved effective, with an increased number of attempts to quit smoking.

[8] Conner, M., and P. Norman (eds.), 2015, Predicting health behavior: research and practice with social cognition models, Open University Press
[9] Thaler, R. H., and C. R. Sunstein, 2009, Nudge: improving decisions about health, wealth, and happiness, Penguin Books
[10] Sunstein, C. R., 2006, Boundedly rational borrowing, University of Chicago Law Review 73:1, 249-270

- **Reminders:** implementing a series of prompts via email or text messages are difficult for consumers to ignore (addressing the omission bias). Scientists have highlighted how delegating a task to an automation device can reduce cognitive load, making it easier for people to act when needed. This has proved effective in different scenarios, such as savings management and medical treatment adherence.[11]

For this to yield anticipated results, customers would need to be assured of clear guardrails, whereby lenders would only be allowed to use such self-disclosed information for the purpose of assisting customers with the disclosed vulnerability rather than by gifting lenders ammunition to penalize customers for an elevated risk. Potential examples of assistance from the lender could include using the right communication channels, indicating the right products, or suggesting repayment holidays. To put customers at ease, lenders could be legally obliged (or pledge) to offer those self-disclosing a vulnerability a similar treatment to that afforded to the British "legally protected characteristics", which cannot be discriminated against.[12] In this way, those flagging their vulnerabilities would be exempted from penalties. On the flipside, they could be subjected to the usual penalizing procedure if they failed to flag their vulnerability and ended up in arrears – that is in the eventuality that the lenders wished to apply a "carrot and stick" approach.

3.2 How to technically capture, manage, and store this data to ensure compliance with Consumer Duty regulation

Given that managing risks is right at the center of the lenders' business, when it comes to their customers' vulnerabilities, inferring these issues is problematic, as it introduces uncertainty into the lender's risk management. Self-disclosures would help lenders pre-empt, or mitigate, problems arising from their clients ending up in arrears and be positive for their risk management.

Another issue is brand management and PR, as lenders are typically well-known and respected institutions. For example, if a bank were to build a "natural language processing" (NLP) model aimed at inferring vulnerability, it should disclose that fact to customers to comply with data processing laws, such as GDPR, and in general to keep everything regarding their relationship with their customers "above board". Such a disclosure could be perceived as "bad optics" from a PR perspective. Additionally, the consequences of getting such an NLP model wrong and inferring vulnerabilities where there are not any, or misdiagnosing them, would carry a further significant reputational risk for the lender. That is another apparent reason why banks should prefer self-disclosure by clients, given their precision and cost effectiveness.

A separate question is whether financial institutions are sufficiently empowered to help customers who flag vulnerabilities. That is important from the customer experience angle, as a customer who self-discloses but does not receive appropriate support would not only be disappointed but could also lodge complaints and be deterred from flagging their vulnerabilities in the future. Any potential penalization resulting from such a self-disclosure would create a bad customer experience.

Not just lenders, but ancillary enterprises, such as credit scoring agencies, should also positively perceive people self-identifying their potential or expected vulnerabilities. Such self-awareness on the customers' part would prove that they are responsible individuals, particularly when faced with the tightening of their finances, the resulting reduced spending, the need to make difficult lifestyle choices, and so on. While there are benefits to the wider financial services industry resulting from the empowerment of customers to self-disclose their vulnerabilities, evaluation of the wider impact is beyond the scope of this article.

It is also worth noting that, due to the breadth of vulnerabilities in scope of Consumer Duty (as visualized in Table 1) lenders may find that one solution will not fit all potential disclosures and there may be a need for a variety of approaches.

In this paper, two approaches are explored to solve the above-mentioned issues. The first is a data lake, selected due to its current wide usage in the financial services industry. The second is blockchain, selected due to the expected benefits and advantage it can deliver in the future. By comparing them, we aim to understand their limitations and potential when used to facilitate compliance with the Consumer Duty regulation.

[11] Gravert, C., 2019, "The hidden costs of reminders," Behavioral Scientist, March 19, https://tinyurl.com/dcnddxd3. Orbell S., S. Hodgkins, P. Sheeran, 1997, "Implementation intentions and the theory of planned behavior," Personality and Social Psychology Bulletin 23:9, 945-954

[12] Gov.uk, 2010, "Discrimination: your rights," U.K. Government, https://tinyurl.com/yj4328tz

A data lake is a centralized repository in which raw data are stored in a structured, semi-structured, or unstructured way, and it is the most common tool used by organizations to store and analyze data. It is designed to handle large amounts of data and is, therefore, a valuable tool for organizations looking to analyze and extract insights from their data in cases where traditional relational databases are not well-suited due to scalability and data variety issues. To address customer vulnerability disclosure, a data lake can serve as a foundational data infrastructure for financial organizations to collect, store, integrate, analyze, and report on customer vulnerabilities, while incorporating robust security and data governance measures.

Blockchain is a decentralized and distributed repository where data are stored in a structured way. By recording transactions across multiple computers, it provides a tamper-resistant and trustless environment that ensures security, transparency, and immutability of the data. This technology, often associated with cryptocurrency and praised for its security features, has become quite popular within the financial services sector, with a compound annual growth (CAGR) of 62.7%[13] since 2016 – and its growth is not expected to halt.[14] To address customer vulnerability disclosures, blockchain ensures the integrity and authenticity of the data, as once a disclosure is made it is securely and permanently recorded, reducing the risk of data manipulation or tampering.

Table 2: Evaluation of the application of data lake technology considering Consumer Duty requirements

FCA REQUIREMENTS	EVALUATION OF THE APPLICATION OF DATA LAKE TECHNOLOGY
1.16 which requires "firms to consider the needs, characteristics and objectives of their customers – including those with characteristics of vulnerability – and how they behave, at every stage of the customer journey." – raising the bar of consumer protection required of the regulated companies. **8.5** which highlights that "many respondents queried the practical application (…) considerations relating to potential vulnerabilities; and the proposed approach to testing communications" – thereby proving the interest expressed by those consulted in the practicalities of flagging up potential vulnerabilities.	When evaluating the application of a data lake with reference to FCA requirements, such a solution would meet para. 1.16 as much as any comparable technology, while not falling foul of para. 8.5 because a data lake does not come across as a relevant tool for capturing vulnerability data itself.
10.6 presents the view of the consumer organizations which "suggested that firms should be required to take an inclusive design approach to meet the needs of customers with characteristics of vulnerability" – hence clarifying the user requirement with regards to the functionalities for flagging potential and actual vulnerabilities.	It would, however, fail the test of para. 10.6 because the data lake managed by a lender would not be particularly inclusive from the perspective of the customer sharing their vulnerabilities.
Annex B 2A.7.4 G specifies that "in relation to the needs and characteristics of retail customers, a firm should, among other things: (…) **(4)** assist frontline staff to understand how to actively identify information that could indicate vulnerability and, where relevant, seek information from retail customers with characteristics of vulnerability that will allow staff to respond to their needs;"[15] – thereby clarifying the requirement for the vulnerability flagging functionality from the point of view of the financial institutions, as well as	In terms of Annex B 2A.7.4 G (4), this technology would not fall foul here, just as much as in para. 8.5, as the data lake would not be used for the purposes of identification of vulnerabilities. However, it must be noted that in reference to not falling foul of the requirements set out by the FCA in both these paragraphs, the application of a data lake is "not applicable".
"**(5)** set up systems and processes in a way that supports and enables retail customers with characteristics of vulnerability to disclose their needs;"[15] – hence providing a further clarification on the user requirement with respect to the same functionality.	A data lake could not be used to help customers with their disclosures as it relies for its data on inputs from other systems, which by its nature would be logistically difficult to be performed by individual customers who simply wish to input their vulnerability information into a user interface.

[13] https://tinyurl.com/2s3asmem
[14] https://tinyurl.com/2p9s5ad2
[15] FCA, 2022, "A new Consumer Duty, Feedback to CP21/36 and final rules," Policy Statement PS22/9, July, Financial Conduct Authority, https://tinyurl.com/yw6mm3p

4. SOLUTION EVALUATION

4.1 Data lake technology evaluation

It may be tempting to frame the solution as a data lake use case. Banks are by now well serviced in this regard by competing "cloud services providers" (CSPs) and typically well-versed in the use of this technology. Extending existing data lakes' application to cover self-disclosures of customer vulnerabilities may, therefore, appear as a logical next step to take.

To summarize, as far as the FCA's requirements for a vulnerability self-disclosure solution are concerned, data lake technology falls on two separate accounts and is not particularly applicable to another two.

With GDPR in mind, inspection by an individual (required by law) of the data held about them by their lender in a data lake would require a customer request that would need to be fulfilled by staff working for the lender running appropriate queries in the data lake. That again, would not bode well for the transparency and timeliness, and hence, in the light of the argumentation above in the "customer's considerations" section, would not provide for an encouraging environment for vulnerabilities self-disclosures. Lastly, regarding the behavioral science aspects mentioned above, the data lake does not appear to contribute vastly to creating an environment stimulating self-disclosures, as there does not seem to be a major improvement in transparency with the lenders simply gaining another tool to manage their customers' data.

4.2 Blockchain technology evaluation

We have explored limitations of the data lake and to obtain a more holistic perspective would also need to evaluate blockchain for this use case.

In this case, specific customer data collection with regards to a particular product (such as a mortgage) could be managed on a single chain throughout the product's lifetime. Due to privacy concerns and relevant data protection laws, the transparency inherent within blockchain, which allows anyone to be able to inspect it, would need to be curtailed. That, however, is not a problem, as private blockchains – visible only to predefined parties – are already in use across several industries. In this case, a private blockchain could be utilized and designed in such a way that only the customer, the lender, and, if relevant, a mortgage broker, personal financial adviser/wealth manager, and, perhaps, the credit scoring agency could access the information held on the chain; with the ability to write further restrictions as necessary. Particularly with credit scoring agencies in mind, smart contracts representing events in the customer's history and stored on the blockchain could provide data-backed evidence on how this customer has handled their vulnerabilities before.

Interestingly, since the major CSPs – including Azure, AWS, and GCP – provide not just data lake but also blockchain solutions, banks, who are heavily invested in their data lakes, could potentially build on these with blockchain in a way that one technology could complement the other for the purpose of managing their customers' vulnerability self-disclosure data.

Table 3: Evaluation of the application of blockchain technology considering GDPR requirements

GDPR REQUIREMENTS	EVALUATION OF THE APPLICATION OF BLOCKCHAIN TECHNOLOGY
Art. 13 GDPR "Information to be provided where personal data are collected from the data subject"[16]	Meets this article as smart contracts could be set up in a way that all the GDPR-required information would be provided to the data subject (i.e., customer flagging their vulnerability).
Art. 14 GDPR "Information to be provided where personal data have not been obtained from the data subject"[17]	In the event that vulnerability-related data stored on blockchain relating to the data subject were obtained via another party, the smart contract could be set up in a way that it would inform the customer of all the information required by GDPR.
Art. 15 GDPR "Right of access by the data subject"[18]	This is the area where the application of blockchain would have the clearest advantage over the application of data lake because it would offer the data subject the ability to instantly inspect data held on them by the data controller (i.e., the lender).

[16] https://tinyurl.com/4xzbuutw
[17] https://tinyurl.com/a9ancxcu
[18] https://tinyurl.com/bdcmbmym

At first glance, the unrestricted transparency that comes with the use of public blockchain (in contrast to private blockchain proposed here) might make the application of this technology to managing self-disclosures of customers' vulnerabilities appear to go against the requirements of GDPR. As such, one may overlook the fact that it enables instant inspection of personal data held by the lender. Consequently, such a facility would in turn be very much GDPR-compliant. In fact, the use of blockchain would help the solution to meet GDPR articles as outlined in Table 3.

As such, it seems fair to say that blockchain does contribute to an increase in transparency and helps build an environment where customers should feel more comfortable to self-disclose their vulnerabilities. It also scores higher in terms of the aforementioned behavioral science criteria than a data lake solution.

Table 4: Evaluation of the application of blockchain technology considering Consumer Duty requirements

FCA REQUIREMENTS	EVALUATION OF THE APPLICATION OF BLOCKCHAIN TECHNOLOGY
1.16 which requires "firms to consider the needs, characteristics and objectives of their customers – including those with characteristics of vulnerability – and how they behave, at every stage of the customer journey." – raising the bar of consumer protection required of the regulated companies. **8.5** which highlights that "many respondents queried the practical application (…) considerations relating to potential vulnerabilities; and the proposed approach to testing communications" – thereby proving the interest expressed by those consulted in the practicalities of flagging up potential vulnerabilities.	Evaluating the application of blockchain in the light of the relevant FCA requirements, as listed in the "Introduction", similar to the above data lake assessment, also here both the paragraphs 1.16 and 8.5 are met, as in either case, the new technologies help firms to better consider the characteristics of vulnerability of their customers and assist these customers with flagging up their vulnerabilities. However, blockchain could offer more with respect to communicating with the customer with regards to their vulnerabilities, as the fact that it allows all parties to write to it means it is more interactive than a data lake, which would be managed by the lender with inputs from other systems and the customer only allowed a limited insight.
10.6 presents the view of the consumer organizations which "suggested that firms should be required to take an inclusive design approach to meet the needs of customers with characteristics of vulnerability" – hence clarifying the user requirement with regards to the functionalities for flagging potential and actual vulnerabilities.	Blockchain meets para. 10.6, as it allows the customer to write directly to the blockchain as well as to inspect in real time everything stored on it with regards to their data. It is more interactive and transparent, and, therefore, ticks the box of the "inclusive design approach", which the FCA specifically points to.
Annex B 2A.7.4 G specifies that "in relation to the needs and characteristics of retail customers, a firm should, among other things: (…) **(4)** assist frontline staff to understand how to actively identify information that could indicate vulnerability and, where relevant, seek information from retail customers with characteristics of vulnerability that will allow staff to respond to their needs;" – thereby clarifying the requirement for the vulnerability flagging functionality from the point of view of the financial institutions, as well as	With regards to Annex B 2A.7.4 G (4), unlike in the case of the data lake, the fact that the vulnerable customers would use blockchain functionality to self-disclose and classify their problems means that it would assist frontline staff in identification of the information pertaining to these self-disclosed vulnerabilities.
"**(5)** set up systems and processes in a way that supports and enables retail customers with characteristics of vulnerability to disclose their needs;"[19] – hence providing a further clarification on the user requirement with respect to the same functionality.	Similarly, for 2A.7.4 G (5), also unlike the data lake, blockchain would help the customers self-disclose their vulnerabilities by allowing them to write directly to the chain.

[19] https://tinyurl.com/yw6mm3p

5. CONCLUSION

In summary, the application of blockchain is the more appropriate solution to fulfill the FCA requirements with regards to vulnerability self-disclosures and complies with GDPR considerations. Blockchain enables the real-time capture of data directly from clients to create the data record at source (including future updates driven by changes in the client/consumer's personal circumstances). It provides the lender with the ability to proactively seek client information updates (through the application of smart contracts) as well as full auditability of the client/consumer data throughout the full product lifecycle and/or existence of the client relationship. It offers full and flexible control of the data through consensus and permissions by all participants in the chain (including the consumer). It fully supports consumer access to their data (in full compliance with GDPR) in a timely manner. Blockchain is also able to support the end-to-end client lifecycle management process through a single blockchain, removing the need to manage different stages of the process across multiple and disparate systems (leading to data integrity and quality issues).

Data lakes can also be considered as a valid solution and may have an advantage over blockchain as they are widely employed by financial services organizations today. However, the key disadvantage is that the data lake architecture tends to remove financial services organizations' proximity to client facing technology, which is required to capture client data and, therefore, makes it challenging to integrate valuable customer information with the same efficiency as blockchain.

Consequently, blockchain is the more transparent and inclusive option as it can allow the customer to write directly into it, enabling immediate inspection and, thereby, stimulating an honest, open dialogue between the parties.

Image generated by Adobe Firefly

As such, the behavioral science guidelines presented to empower the customers to self-disclose are also better fulfilled by blockchain. Today, the minimal penetration of traditional financial services by blockchain technology is a clear obstacle when it comes to adoption, as it may make this solution less cost effective than a data lake, even if the data lake does not meet all of the FCA's objectives with regards to the vulnerability self-disclosures set out in the Consumer Duty regulation. However, the analysis and assessment contained in this paper brings to light an innovative blockchain "use case" that financial services organizations should consider developing to facilitate and enhance their compliance with the Consumer Duty regulation.

ABOUT CAPCO

Capco, a Wipro company, is a global technology and management consultancy focused in the financial services industry. Capco operates at the intersection of business and technology by combining innovative thinking with unrivalled industry knowledge to fast-track digital initiatives for banking and payments, capital markets, wealth and asset management, insurance, and the energy sector. Capco's cutting-edge ingenuity is brought to life through its award-winning Be Yourself At Work culture and diverse talent.

To learn more, visit www.capco.com or follow us on Facebook, YouTube, LinkedIn and Instagram.

WORLDWIDE OFFICES

APAC
Bangalore – Electronic City
Bangalore – Sarjapur Road
Bangkok
Chennai
Dubai
Gurgaon
Hong Kong
Hyderabad
Kuala Lumpur
Mumbai
Pune
Singapore

EUROPE
Berlin
Bratislava
Brussels
Dusseldorf
Edinburgh
Frankfurt
Geneva
London
Milan
Munich
Paris
Vienna
Warsaw
Zurich

NORTH AMERICA
Charlotte
Chicago
Dallas
Hartford
Houston
New York
Orlando
Toronto
Washington, DC

SOUTH AMERICA
Alphaville
São Paulo

THE COVER IMAGE WAS CREATED USING JASPER AI, AN AI ART GENERATOR

FSC
www.fsc.org
MIX
Paper from responsible sources
FSC® C004309

WWW.CAPCO.COM

CAPCO 25
a wipro company