Technology System Stability in Financial Services Regulatory Programmes

ABSTRACT

This work is a quantitative research on Major Programme Management and financial services technology systems. It investigates the relationship between consecutive and concurrent regulatory programmes in the financial services sector and the impact on the stability of its technology systems. While programmes are typically measured in terms of meeting planned budget, schedule and desired deliverables, systemic outcomes are typically ignored. To facilitate the research, the United Kingdom (UK) outage data from Ookla's Downdetector is used. UK and European regulators did not provide the required data for this research.

The research covers Event Analysis, Complexity and IT Architecture. Downdetector data analysed includes 2983 outages between 2015 and 2021 from 43 UK financial institutions. The data shows that regulatory programmes impact the stability of technology systems in the form of increased service outages especially as the deadlines for regulatory programmes converge closer together. The research concludes with recommendations and further work to push the current research boundaries.

Keywords: regulation; stability; programme; management; technology; finance

Statements and Declarations

The author has no relevant financial or non-financial interests to disclose. The author conducted this research at the Said Business School, University of Oxford and is grateful for the supervision of Dr. Alexander Budzier. The views expressed herein are those of the author and do not necessarily reflect the views of the National Bureau of Economic Research.

Introduction

The regulation of the Financial Services sector in response to 2008 financial crisis has resulted in organisations running concurrent and consecutive regulatory programmes to be in compliance with new industry regulations. Macroprudential regulation is the means by which regulators mitigate risk in the financial system by focusing on the entire system rather than on individual firms. This research aims to consider how these regulatory programmes cumulatively impact the financial services sector. The impact has been measured against the stability of the technology systems that not only enable the sector but usually incorporate adjustments in response to regulatory changes.

Major programmes, including regulatory programmes, are plagued with the well-known Iron Law that makes it difficult to control such programme costs, schedule and desired outcomes (Flyvbjerg, 2014). Putting these together, we see that regulators enact regulations, and financial institutions run programmes to be compliant with those regulations. These programmes are subject to Iron Law which mean they do not always give the desired outcomes. Cost and schedule overrun of IT programmes have been well studied (Flyvbjerg, et al., 2022), while benefits of such programmes have not. A key element of the benefits of IT systems is adoption and system quality (Sabherwal, et al., 2006). Operational incidents are an important measure of the system quality. They affect the stability of the technology systems which consequently affect the stability of the financial systems they operate in.

An illustration of the instability of these technology systems is a survey by the Financial Conduct Authority (FCA) which confirmed the number of reported incidents over a year increased by 187% (Financial Conduct Authority, 2018). The report showed that technology outages have become more frequent and publicly impacting in the Financial Services sector. It

revealed that failed change management is the major cause of incidents and alone accounted for 20% of operational incidents reported. It was silent on the proportion of these change management incidents that are based on regulatory programmes. This research gives a different perspective on the possible root of these issues and it investigates how they could be more systemic than they appear to be.

The core research question this paper aims to answer is to determine if Financial Services regulatory programmes impact UK technology system stability.

Theoretical Background

A critical foundation to understanding the arguments of this work is to know the type of system that financial markets are. Financial systems are a collection of banks, insurance companies and other institution which facilitate the exchange of funds for lenders, borrowers and investors. Financial systems are complex systems (Johnson, et al., 2003). Complex systems are non-linear such that it can be difficult to correlate cause and effect (Cicmil, et al., 2009, p. 69). Their emergent nature means that the properties exhibited by the system cannot be accounted for by individual components that make it up. This is why governments have struggled to both predict and control their financial systems with market crashes happening repeatedly over decades. In certain cases, the effects of new policies are not realised until many years later and it might be too late to avert the negative consequences of such policies. These have informed a change in strategy as regulators approach their function from a macroprudential perspective where they focus on the stability of the entire system rather than just the stability of individual financial institutions (Chapman, 2012; Harnay & Scialom, 2016; Loesch, 2018, p. 18).

Financial institutions run projects or programmes to remain in compliance with regulatory changes especially after the 2008 financial crisis. The number of these regulatory changes mean that institutions can run them concurrently and consecutively. While all may not be regulatory related, it is reported that some large institutions run hundreds or thousands of change programmes concurrently (TheCityUK, 2019, pp. 38-40). It was predicted that between 2017 and 2022, compliance costs could more than double from 4% to 10% of revenue for financial institutions (Bouyon, 2018, pp. 10, 19). All categories of IT spending by banks in Europe, North America and Asia-Pacific for 2015 was estimated to be $197 billion (Jegher et

al, 2015 cited in Bouyon, 2018, p. 12). Naturally, technology systems are at the receiving end of regulatory changes. Technology systems are the backbones of our financial systems.

These regulatory programmes are subject to Project Management Triangle or Iron Law of Major programmes (Flyvbjerg, 2014). Regular projects become Major programmes when the methodologies of the former are no longer effective for the latter. This is because major programmes exhibit the properties of complex systems (Cicmil, et al., 2009, pp. 3, 7, 9-10). Hence, to understand the effects of regulatory programmes on the financial system, which is itself complex, one must have an idea about the properties of complex systems.

The re-regulation of the financial services sector after the 2008 financial crisis is a 'trait making' endeavour because technology is a major ingredient at a scale that didn't exist in previous crises (Flyvbjerg, 2017, p. 3; Pierri & Timmer, 2021). For the regulators, that becomes a major programme with added complexity to manage when we consider that regulators actually run the major programmes in financial services that drive the sector.

What system characteristics are associated with operational incidents: legacy or new systems, within or across banking groups as a result of domino effects? The response of systems to changes depends on the nature of these systems especially if they have legacy or modern architectures. Legacy systems are generally more difficult to manage and many financial institutions are still burdened with them (Hall, 2019, p. 24; Comella-Dorda, et al., 2000; Darolles, 2016, pp. 88-89; Abusdal & Gjermundnes, 2019, p. 61).

Making software changes to critical legacy systems that require a high availability uptime is challenging. To keep the systems running, changes have to be made in several small increments and project management abilities are required in addition to software engineering (Ronzon, 2016). These systems become legacy especially in risk averse financial services institutions (Anagnostopoulos, 2018, pp. 13-14) where no one touches it till it breaks or the world around it forces change (Gill, 2011, p. 43; Robinson, 2011, pp. 71-72). Some software changes have resulted in customer impacting multi-day service outages and got the attention of industry regulators (Financial Conduct Authority, 2018). Banks such as Barclays Bank admit that regulatory requirements mean they do system upgrades that require system downtime (Munbodh, 2018).

To effectively manage the financial services sector, regulators must understand the system of systems. In this case, they need to monitor how their regulations affect the sector and also keep an eye on how technology systems which power the sector are impacted as a subsystem. The Year 2000 IT date glitch (Y2K) review indicated to financial institutions their technology dependence and the domino effects of that dependence to other market participants (Raghavan, 2007, p. 183) (Darolles, 2016, p. 91). This background helps to accommodate unplanned and undesired outcomes that could emerge from regulatory programmes in form outliers or black swan events (Taleb, 2010, p. 17).

We can consider how many organisations meet regulatory requirements with in-house solutions and those that rely on external vendor solutions or banking-as-a-service partnerships. Organisations' sizes can be grouped based on number of employees to check if bureaucracy affects technology change. Finally, we can group firms by the number or types of licenses they operate with, universal banks or boutique finance firms, revenue size and small local or big

multinational firms. We can perhaps gauge organisation complexity and legacy based on the number of customers and age of the organisation.

Regulatory changes require business process adjustments to be implemented on technology systems shared by various subsidiaries of the same financial institutions. Organisations are described as a system of interlinked processes (Benner & Tushman, 2003, p. 238). Financial services conglomerates that run insurance and banking groups could share the same treasury and IT systems (Loesch, 2018, p. 25). For such cases, it implies that regulatory changes for the insurance subsidiary affects the banking one and vice versa. This suggests that these regulatory programmes may have larger system scopes and consequently, more systemic implications (Darolles, 2016, pp. 88-89).

On the other hand, there are regulatory changes that cut across all sectors including money laundering, terrorist finance, financial crime, data protection and privacy (Loesch, 2018, p. 31). This raises the question of whether subsidiaries report technology incidents on shared systems, from regulatory changes which they are not subject to, caused by other subsidiaries. PSD2 gives some insights on what regulators request for in terms of incident reporting (European Banking Authority, 2017). We see that the document allows delegated reporting, recognises indirect incidents by service providers, and that these incidents can affect other Payment Service Providers (PSPs).

The FCA's Policy Statement PS17/26 on Operational and Security incidents (Financial Conduct Authority, 2017, pp. 33-34) is based on the major incident framework of PSD2 agreed by regulators across Europe. This framework is a matrix of quantitative and qualitative impact thresholds which categorizes a downtime of over two hours in the low impact level (European

Banking Authority, 2017, p. 23). This downtime threshold of over two hours is considered along with other thresholds before a financial institution is mandated to report to the appropriate European regulator. This threshold allowance for a single incident is two to twenty times what Google allows in an entire year as part of its Service Level Objectives for its "four 9s" and "five 9s" availability services (Gill, 2011, p. 43; Treynor, et al., 2017, p. 42). This bar is low and potentially leaves a lot of customer service pains outside the view of regulators.

The toolkit for macroprudential regulation is data collection and analytics through bespoke reports and stress tests to confirm financial stability of the sector (Loesch, 2018, p. 21). The same approach can be applied to macro-prudentially test technology systems. Macroprudential regulation comes into play when addressing risk/stability at the sector/industry level. It then helps us to look at Globally Systemic Financial Institutions. However, there are challenges in developing robust analytical frameworks to monitor macroprudential policies. Besides the data gaps that exists nationally and internationally for measuring systemic risk, there is no agreed definition of what systemic risk is as it can be very opaque, multifaceted and complex (Chakrabarty, 2014, p. 142). Caruana and Cohen suggest how macroprudential policies have been misused and overburdened (Caruana & Cohen, 2014, pp. 16-19). They use the February 2011 definition by the Financial Stability Board (FSB), International Monetary Fund (IMF) and the Bank for International Settlements (BIS) for macroprudential policy below.

"a policy that uses primarily prudential tools to limit systemic or system-wide financial risk, thereby limiting the incidence of disruptions in the provision of key financial services that can have serious consequences for the real economy." (Caruana & Cohen, 2014, p. 16)

Caruana and Cohen also emphasized the importance of looking out for spill overs that result from macroprudential policies. This research does that for technology systems. They also opine that macroprudential polices address systemic risks that occur in the time dimension and the cross-sectional dimension. Time dimension focuses on the financial imbalances that happen over time while the cross-sectional dimension looks at risks and interdependencies across firms, markets and sectors (Caruana & Cohen, 2014, p. 17).

Knot went further to state that while tracking systemic risk is difficult and strong governance frameworks help, there are no guarantees that macroprudential policies work (Knot, 2014, p. 31). He recommends finding the right balance between the time-varying macroprudential policy tools and the structural (cross-sectional) ones which are less prone to inaction bias as they are not primarily time dependent. While the efficacy of macroprudential tools is uncertain, Knot recommends that financial authorities learn from experience. This uncertainty again points to a major attribute of complex systems where the output of the system cannot be guaranteed after a particular input is applied.

Institutions classified as Globally Systemic Important Banks (GSIB) or Globally Systemic Financial Institutions (GSFI) reflect this importance solely based on financial or economic risk metrics rather than the risk exposure from their technology systems. A Swedish research concluded that besides the possibility of important indicators being omitted in measuring GSIB, in practice, systemic risk is too complex to ignore many feedback loops that come into play with financial systems (Bengtsson, et al., 2013, p. 69). Do GSIB/GSIF respond differently to the modifications from regulatory change programmes? Will the stability of GSIBs or GSFIs technology systems affect the sector? Will the results to these questions vary if the GSIBs are assessed as indicator-based or model-based categorisations? This is

particularly difficult because even in the classification of Systemic Important Banks, there is no one size fits all solutions from different countries in the world (Gu & Zhu, 2015).

Conceptual Model

Below is the conceptual model in Figure 2 and hypotheses to be tested for this research work. They have been drawn from the literature.

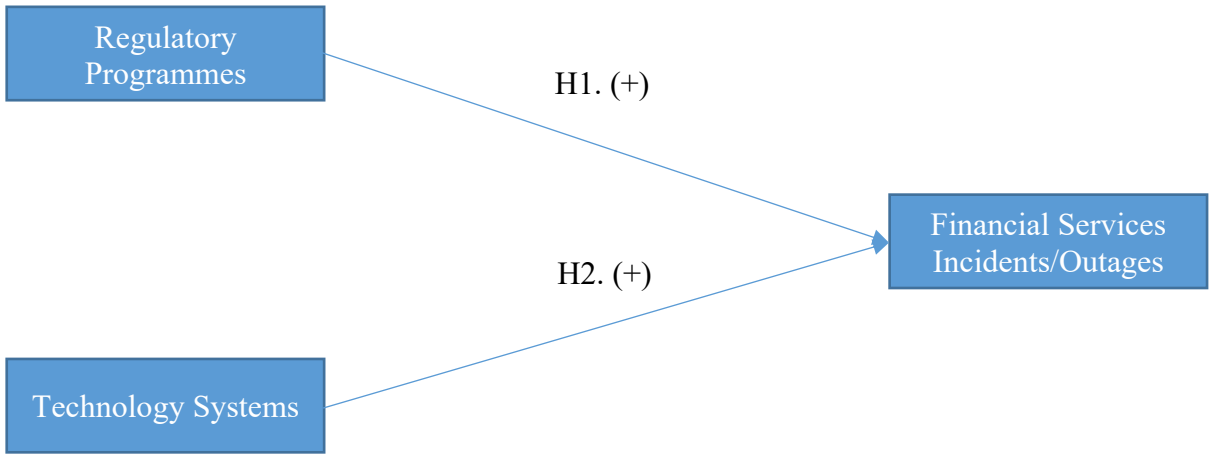


Figure 1 Research Conceptual Model

Research Hypotheses

H1. Do Concurrent and Consecutive Financial Services Regulatory Programmes impact UK technology systems?

H2. Are Legacy Technology systems less tolerant to several business process changes than modern systems?

Research Methodology

The chosen methodology for this research is the quantitative analysis of secondary data similarly used by the FCA (Financial Conduct Authority, 2018). 4 regulators/central banks and a real-time outage tracking company were contacted for research data. These included the Financial Conduct Authority (FCA) which indicated a 187% increase in reported incidents (Financial Conduct Authority, 2018). Others are the Bank of England (BoE) which houses the Prudential Regulation Authority (PRA), the European Banking Authority (EBA), and the European Central Bank (ECB). The company that tracks outage data is Ookla's Downdetector.

A major gap in the FCA report is an account of how many IT change failures are a result of regulatory-originated transformation programmes (Financial Conduct Authority, 2018). Running a major programme is challenging but running several of those, especially on legacy technology, is systemic and could be responsible for the instability of those banking systems. There have been several regulatory changes. Some of these regulatory directives and economic events include Markets in Financial Instruments Directive 2 (MiFid II), PSD2, and General Data Protection Regulation (GDPR) among others. While Figure 1 does not include the expected regulatory changes of Britain leaving the European Union (Brexit) (Moloney, 2018), it highlights 22 regulatory originated programmes over a span of 6 years. See below for the full list of the programmes.

List of Financial Services Regulatory Programmes

Annual Bank Stress Testing

Short Selling Regulation (SSR)

Capital Requirements Regulation (CRR) / Credit Requirements Directive (CRD)

Mortgage Credit Derivative

Bank Recovery and Resolution Directive (BRRD)

Markets in Financial Instruments Directive 2 (MiFid II)

Market Abuse Regulation (MAR) / Market Abuse Directive (MAD)

European Market Infrastructure Regulation (EMIR)

Senior Managers and Certification Regime (SM&CR)

Deposit Guarantee Schemes Directive (DGSD)

Central Securities Depositories Regulation (CSDR)

4th Anti Money Laundering Directive (4AMLD)

Securitisation Regulation

Securities Financing Transactions Regulation (SFTR)

Payment Services Directive 2 (PSD2)

Operational Continuity in Resolution (OCIR)

General Data Protection Regulation (GDPR)

Banking Reform Act 2013 (Ring Fencing)

European Benchmarks Legistlation

Fourth Basel Accord (Basel IV)

EBA Guidelines for IRRBB (Interest Rate Risk in the Banking Book)

London Interbank Offered Rate (LIBOR) transition

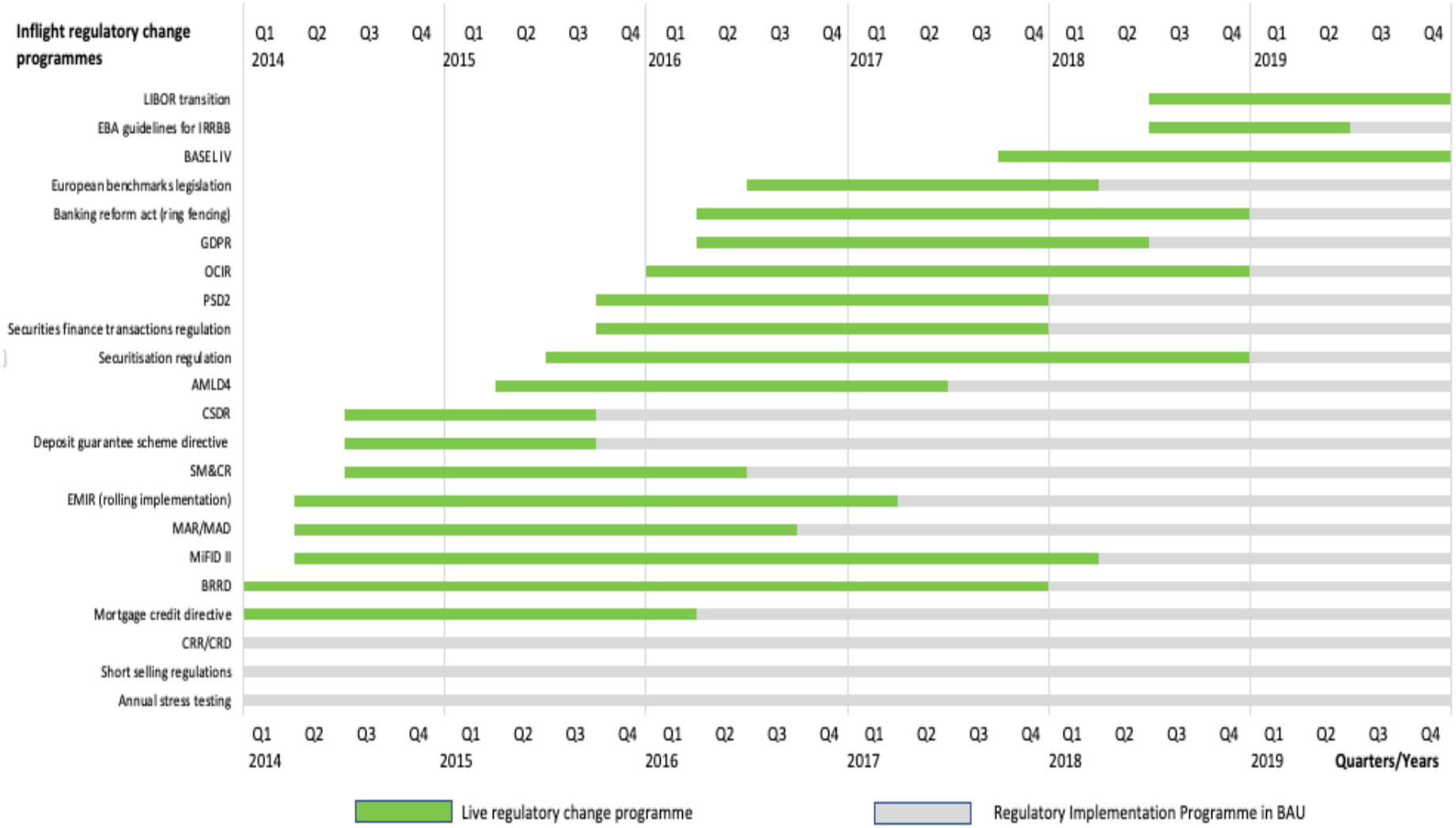


Figure 2 Banking regulatory change programmes. Adapted from TheCityUK (TheCityUK, 2019, p. 39)

A Data Request document was prepared for each organisation and customised slightly differently. There is a significant difference with Ookla's Downdetector data request document because it is not a financial services expert. The provided data was to be in Microsoft Excel or Comma Separated Values (CSV) files. The Data Request document gave the regulators or organisations the option to aggregate data and/or anonymise the names of institutions to protect participants, researchers and stakeholders (Maylor, et al., 2017, pp. 239-241). It gave the option that the researcher takes care of anonymisation to protect participants from being liable for providing potential material information. This is important for the neutral position central banks or regulators occupy.

The Data Request document touches on timelines before and after the 2008 financial crisis, legacy and modern systems, in-house and vendor solutions, Globally Systemic Financial institutions, UK only and international institutions. Central banks and regulators know which regulatory programmes each financial institution participated in. This is crucial for accurate statistical evaluations of data. Redundancies built into technology systems mean certain outages do not affect customers and consequently, outside the view of Downdetector. More so, Downdetector does not cover the full client spectrum as retail rather than corporate or other sophisticated clients will report to it. Consequently, Ookla's Downdetector data will not cover every type of technology incident. However, it will be interesting to compare the results we find from a non-regulatory body with those possessed by regulators to address FCA's under reporting challenge (Butler, 2018).

Despite contacting central banks and regulators early, the requested data was not provided. Ookla needed to arrange a data license agreement with the University of Oxford for the research to obtain Downdetector data as part of their Data for Good initiative. The legal

agreement takes months to put in place, hence, the Ookla representative advised the research uses their publicly available resources.

For Ookla's Downdetector, a short Python script aggregated customer outage reports from 43 UK institutions that provide financial services. There are more listed but those without outage data were excluded. For these institutions, Downdetector provides the date and time of each outage incident. From October 2015 till July 2021, there is a record of **2983** outages from these 43 UK financial institutions. Table 1 below gives a list of the institutions and number of outages or incidents. This data is also plotted in Figures 3 and 4.

Ookla's Downdetector tracks online service status information, including banking outages among others, by aggregating and analysing live customer complaints (Downdetector by Ookla, 2021). Live customer complaints include issues logged onto the Downdetector website, social media sentiment analysis through Twitter and signals from other websites. Customer outage reports that do not exceed a service baseline level maintained by Downdetector are not recorded as actual incidents against that service or company. To find financial institutions listed on downdetector.co.uk, keywords such as *bank, financial, pay, payment* and *money* where searched. Listed companies without the *Check past issues* links are exempted as ones without Downdetector baselines or previous incidents. Archived issues were observed to follow a URL pattern formed from company, year and month similar to https://downdetector.co.uk/status/barclays/archive/2015/10/. A short Python script was written to aggregate data by looping between shortlisted financial institutions, years 2015 to 2021 and every month of each year.

The aggregated Downdetector data is to be analysed using Microsoft Excel graphs, charts, pivot tables, regression or scatter plots and so on.

Results

Table 1 below gives a list of the institutions and number of outages or incidents. This data is also plotted in Figures 3 and 4.

Figure 4 helps us view the trend of these incidents over time in each year and see a monthly cross-section. Most years, these outages adopt a U-shape where incidents dip by the middle of the year between May and June while it climaxes at the beginning and end of each year. This could be explained as having to do with less regulatory change programmes executed during the summer where most people go on holiday. Or perhaps it is something else entirely. This view makes it appear as though there is a rhythm or heartbeat to our financial services sector. This heartbeat was irregular during the peaks of October 2017 to January 2018.

Table 1 List of UK institutions rendering financial services and recorded outages

UK Financial Institution / Product	Number of Outages
HSBC	**335**
Santander	**326**
Barclays	**318**
Lloyds Bank	**287**
Halifax	**222**
NatWest	**209**
Yorkshire Bank	**194**
TSB Bank	**178**
Nationwide	**165**
The Co-operative Bank	**123**
Paypal	**117**
HMRC	**68**
Tesco Bank	**50**
Bank of Scotland	**47**
First Direct	**46**
RBS (Royal Bank of Scotland)	**46**
Post Office	**39**
Visa	**34**
Metro Bank	**29**
Revolut	**23**
Etoro	**20**
Mastercard	**13**
Sainsbury's Bank	**13**
Monzo	**12**
Barclaycard	**11**
Smile	**11**
DeGiro	**7**
M&S Bank	**6**
Thinkmoney	**6**
Transferwise	**5**
Starling Bank	**4**
Danske Bank	**4**
American Express	**4**
Square	**3**
Sagepay	**3**
Zettle	**2**
Ulster Bank	**2**
Bank of Ireland UK	**1**
Grand Total	**2983**

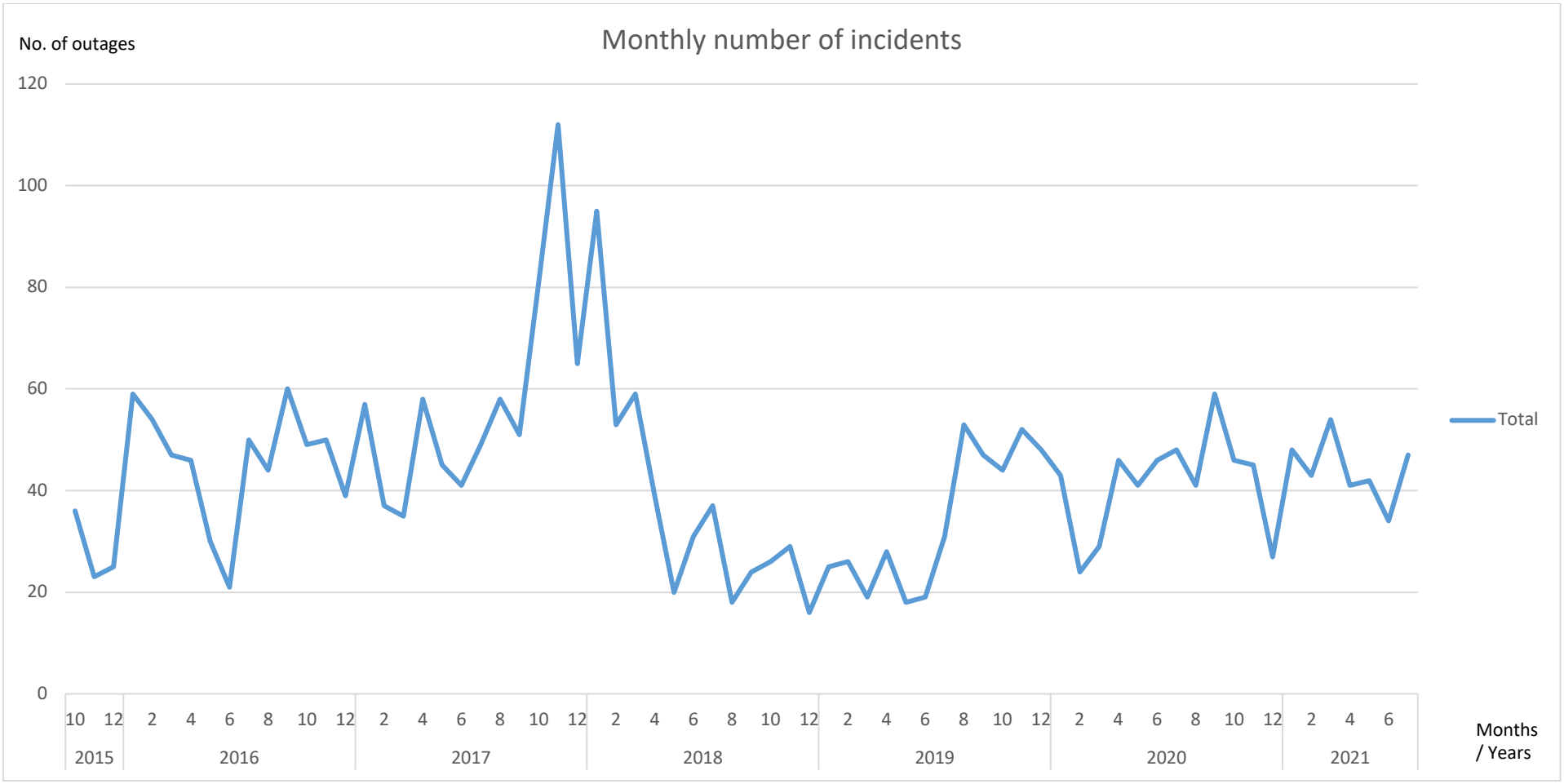


Figure 3 Chart showing the number of technology incidents across the Financial Services Sector

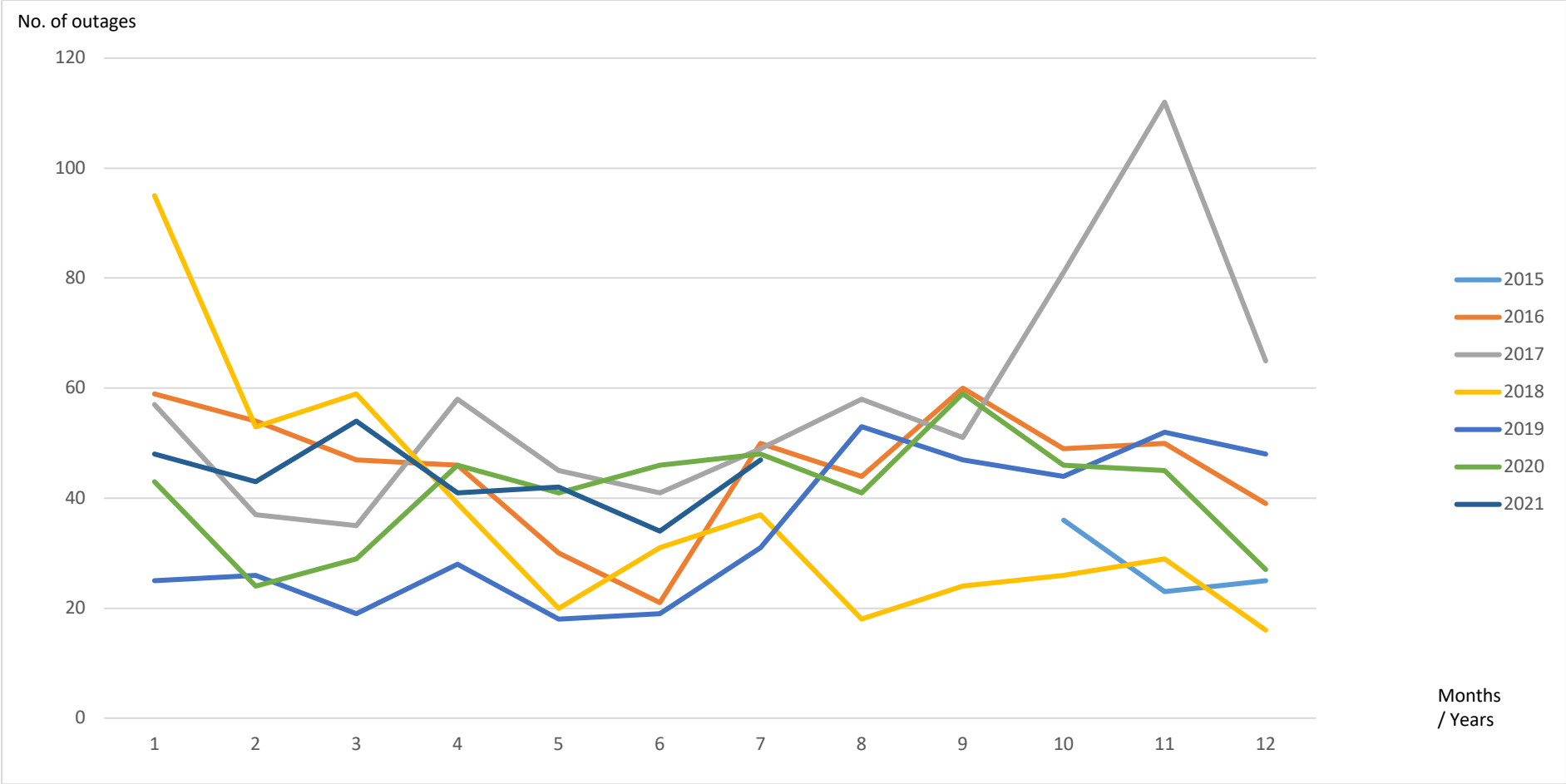


Figure 1 Graph showing annual outages grouped by month of the year

How the number of incidents reported from legacy systems differ from modern ones

We assume that institutions with modern technology are likely to have been established recently, especially when they have no roots in older banks. We review Table 2 and Figure 5 below, which shows each financial institution, total number of outages, age in years, size of UK customer base, incident time range and incidents per time range annually. The incident time range is the time difference in years between the months of the earliest and latest incident record for the institution. The number of incidents per time range annum is an institution's number of incidents divided by the incident time range.

Using Table 2, regressions were plotted but regression charts are non-linear which is expected of a complex system (see Table 3 and Figure 5). That means we cannot use regression. Instead, graphs for a non-linear fit are more appropriate (Figures 6 to 9). In addition, we see that there is a significant positive relationship between the age of the institution and the number of incidents with $p < .001$. This is the same for the relationship between incident range and incidents per annum. The implication is that the results obtained for those are not likely to be solely by chance. However, all other variable combinations with customer base are all statistically non-significant $p < .05$ consistently. This suggests the data obtained for customer numbers is likely solely by chance. It will be useful reviewing those again by obtaining more accurate customer numbers that directly relate to the technology systems that have these incidents.

Table 2 Showing the percentage of incidents, age. customer base, incident time range and incident per time range annually of each financial institution

Institutions	Number of Incidents	Ratio of incident (Percent - %)	Age (years)	Year Established	Customer Base (millions)	Incident Time Range (years)	No of incidents per time range annum
HSBC	335	11.23	185	1836	15.00	5.75	58.26
Santander	326	10.92	17	2004	14.40	5.67	57.53
Barclays	318	10.66	331	1690	24.00	5.75	55.30
Lloyds Bank	287	9.62	256	1765	25.00	5.75	49.91
Halifax	222	7.44	168	1853	0.00	5.75	38.61
NatWest	209	7.00	188	1833	12.50	5.75	36.35
Yorkshire Bank	194	6.50	162	1859	6.00	4.42	43.92
TSB Bank	178	5.97	211	1810	5.00	5.75	30.96
Nationwide	165	5.53	175	1846	16.30	5.75	28.70
The Co-operative Bank	123	4.12	17	2004	0.00	4.75	25.89
Paypal	117	3.92	18	2003	26.00	4.75	24.63
HMRC	68	2.28	172	1849	0.00	2.58	26.32
Tesco Bank	50	1.68	24	1997	5.00	4.67	10.71
Bank of Scotland	47	1.58	326	1695	2.80	5.50	8.55
First Direct	46	1.54	32	1989	1.50	5.67	8.12
RBS (Royal Bank of Scotland)	46	1.54	294	1727	3.00	5.75	8.00
Post Office	39	1.31	6	2015	2.40	4.75	8.21
Visa	34	1.14	55	1966	132.43	2.75	12.36
Metro Bank	29	0.97	11	2010	2.00	5.17	5.61
Revolut	23	0.77	6	2015	12.00	1.58	14.53
Etoro	21	0.70	8	2013	0.00	3.58	5.86
Mastercard	13	0.44	49	1972	26.02	2.58	5.03
Sainsbury's Bank	13	0.44	24	1997	0.00	4.75	2.74
Monzo	12	0.40	6	2015	3.90	1.75	6.86
Barclaycard	11	0.37	55	1966	0.00	0.58	18.86
Smile	11	0.37	22	1999	0.10	3.25	3.38
DeGiro	7	0.23	6	2015	0.63	0.50	14.00
M&S Bank	6	0.20	36	1985	3.50	2.33	2.57
Thinkmoney	6	0.20	20	2001	0.00	1.58	3.79
Transferwise	5	0.17	11	2010	10.00	1.08	4.62
American Express	4	0.13	58	1963	3.21	2.33	1.71
Danske Bank	4	0.13	197	1824	5.00	1.50	2.67
Starling Bank	4	0.13	7	2014	1.50	1.33	3.00
Sagepay	3	0.10	20	2001	0.05	0.75	4.00
Square	3	0.10	4	2017	0.00	0.33	9.00
Ulster Bank	2	0.07	185	1836	1.10	2.00	1.00
Zettle	2	0.07	9	2012	0.00	0.25	8.00
Bank of Ireland UK	1	0.03	38	1983	2.50	0.00	∞

Customer base and age sources: Statista, 2021; UKFinance, 2018; Finder, 2021 and other Google sources

Table 3 Organisation Incidents vs Age

SUMMARY OUTPUT

Regression Statistics	
Multiple R	0.5253481
R Square	0.275990626
Adjusted R Square	0.255879255
Standard Error	90.24995649
Observations	38

ANOVA

	df	*SS*	*MS*	*F*	*Significance F*
Regression	1	111775.506	111775.5064	13.72311314	0.000707198
Residual	36	293221.967	8145.054647		
Total	37	404997.474			

	Coefficients	*Standard Error*	*t Stat*	*P-value*	*Lower 95%*	*Upper 95%*	*Lower 95.0%*	*Upper 95.0%*
Intercept	30.08148733	19.6306315	1.53237492	0.134171697	-9.731278601	69.8942533	-9.7312786	69.8942533
X Variable 1	0.540012755	0.1457732	3.704472045	0.000707198	0.244370997	0.83565451	0.244371	0.83565451

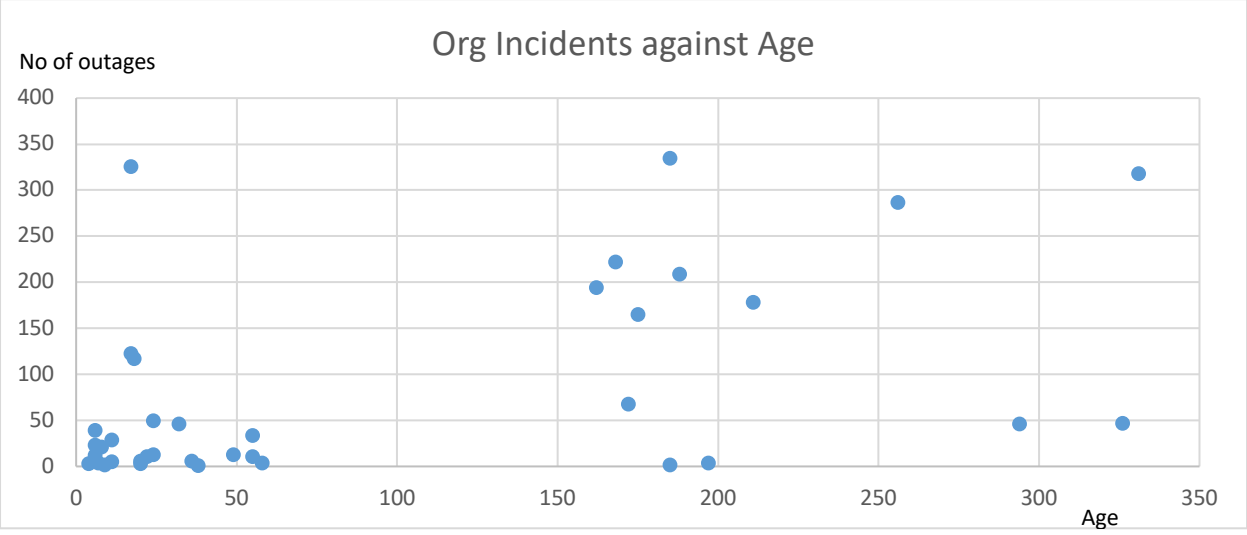


Figure 5 Organisation Incidents vs Organisation Age

The data can be transformed with the log of both variables. That gave balanced distributions for the regressions.

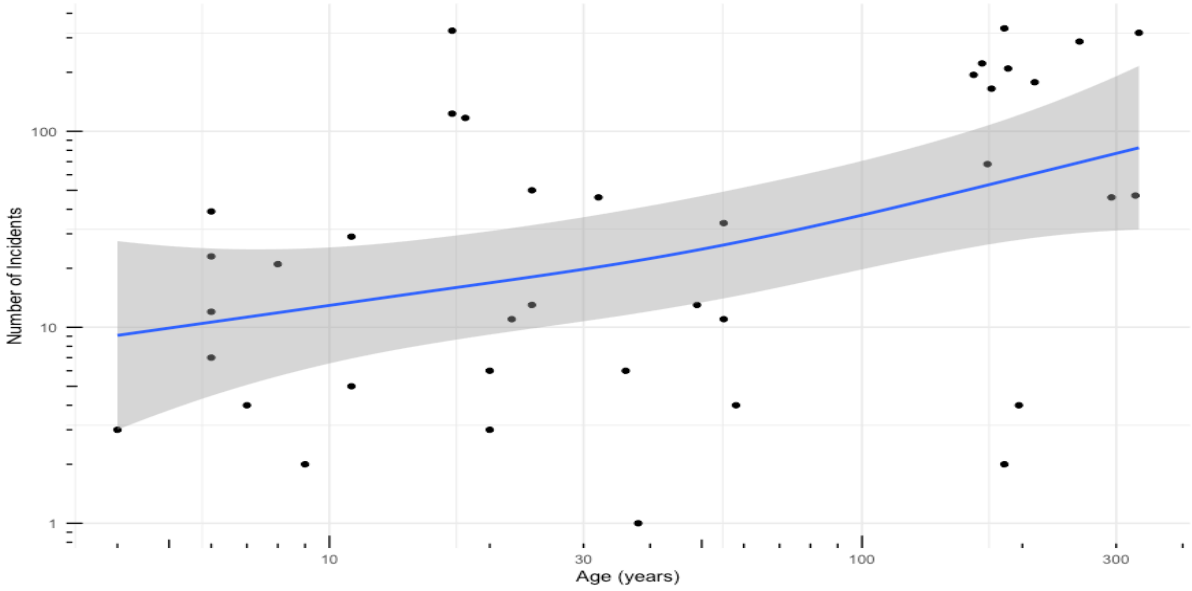


Figure 6 Log of Number of incidents vs Age

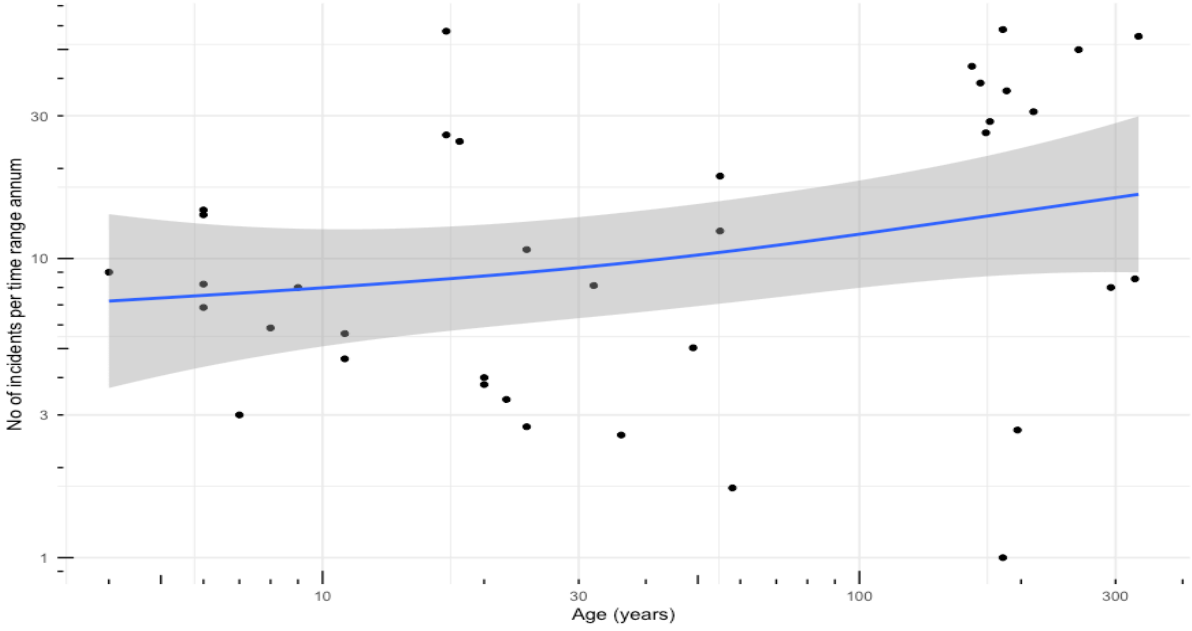


Figure 7 Log of Number of incidents vs Age

Two models fitted to the data using penalized regression splines with restricted maximum likelihood estimation. The age of the financial institution is statistically significant for the number of incidents ($p = 0.00359$) and for the number of incidents per annum in the date range covered for this institution ($p = 0.049$).

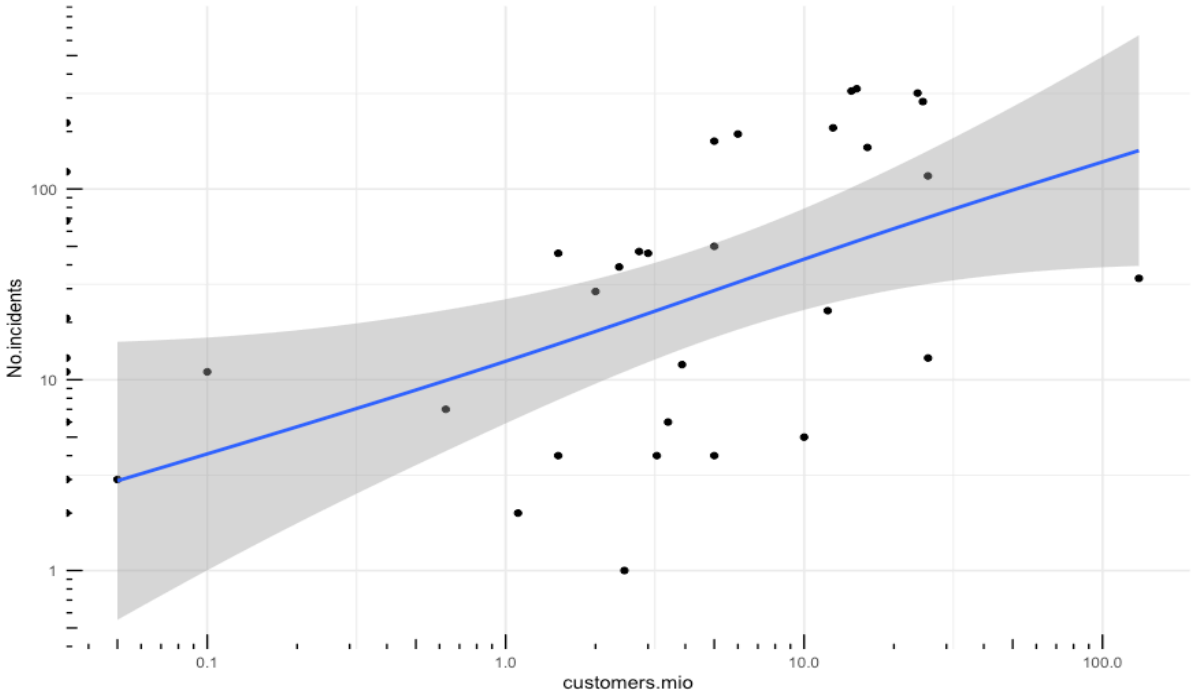


Figure 8 Log of Number of incidents vs Customer Numbers

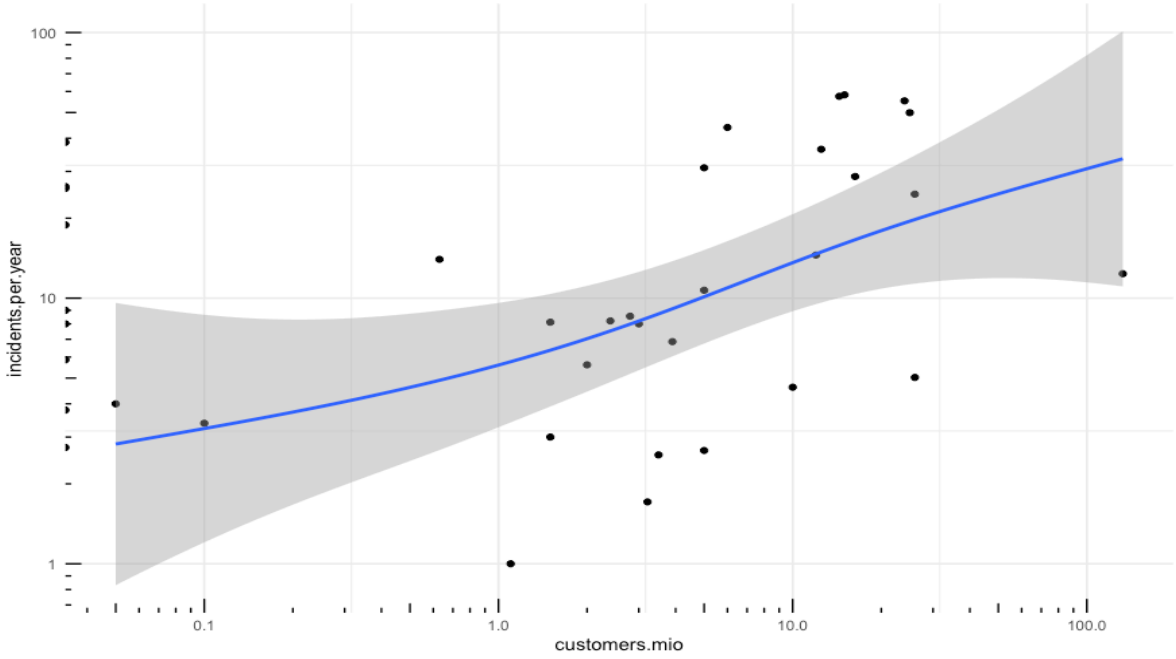


Figure 9 Log of incidents per year vs number of customers

Again tested as above both associations are statistically significant (total number of incidents p = 0.00303; number of incidents per year p = 0.0034).

Taken together in a linear model the customer base is a statistically significantly associated with the number of incidents (p = 0.092) and the number of incidents per year (p = 0.089).

Table 4 Customer Base with Number of incidents

	Estimate Std.	Error	t value	Pr(>|t|)
(Intercept)	1.3560	0.7928	1.710	0.0991 .
log(age)	0.3233	0.2032	1.591	0.1237
log(customers.mio)	0.4917	0.1747	2.814	0.0092 **

Signif. Codes: 0 '***' 0.001 '**' 0.01 '*' 0.05 '.' 0.1 ' ' 1

Residual standard error: 1.455 on 26 degrees of freedom
Multiple R-squared: 0.3532, Adjusted R-squared: 0.3034
F-statistic: 7.098 on 2 and 26 DF, p-value: 0.00347

Table 5 Customer Base with Number of incidents per year

	Estimate Std.	Error	t value	Pr(>|t|)
(Intercept)	1.3864	0.5507	2.518	0.0186 *
log(age)	0.1078	0.1405	0.767	0.4501
log(customers.mio)	0.3436	0.1211	2.837	0.0089 **

Signif. codes: 0 '***' 0.001 '**' 0.01 '*' 0.05 '.' 0.1 ' ' 1

Residual standard error: 1.006 on 25 degrees of freedom
(1 observation deleted due to missingness)
Multiple R-squared: 0.3011, Adjusted R-squared: 0.2452
F-statistic: 5.384 on 2 and 25 DF, p-value: 0.01136

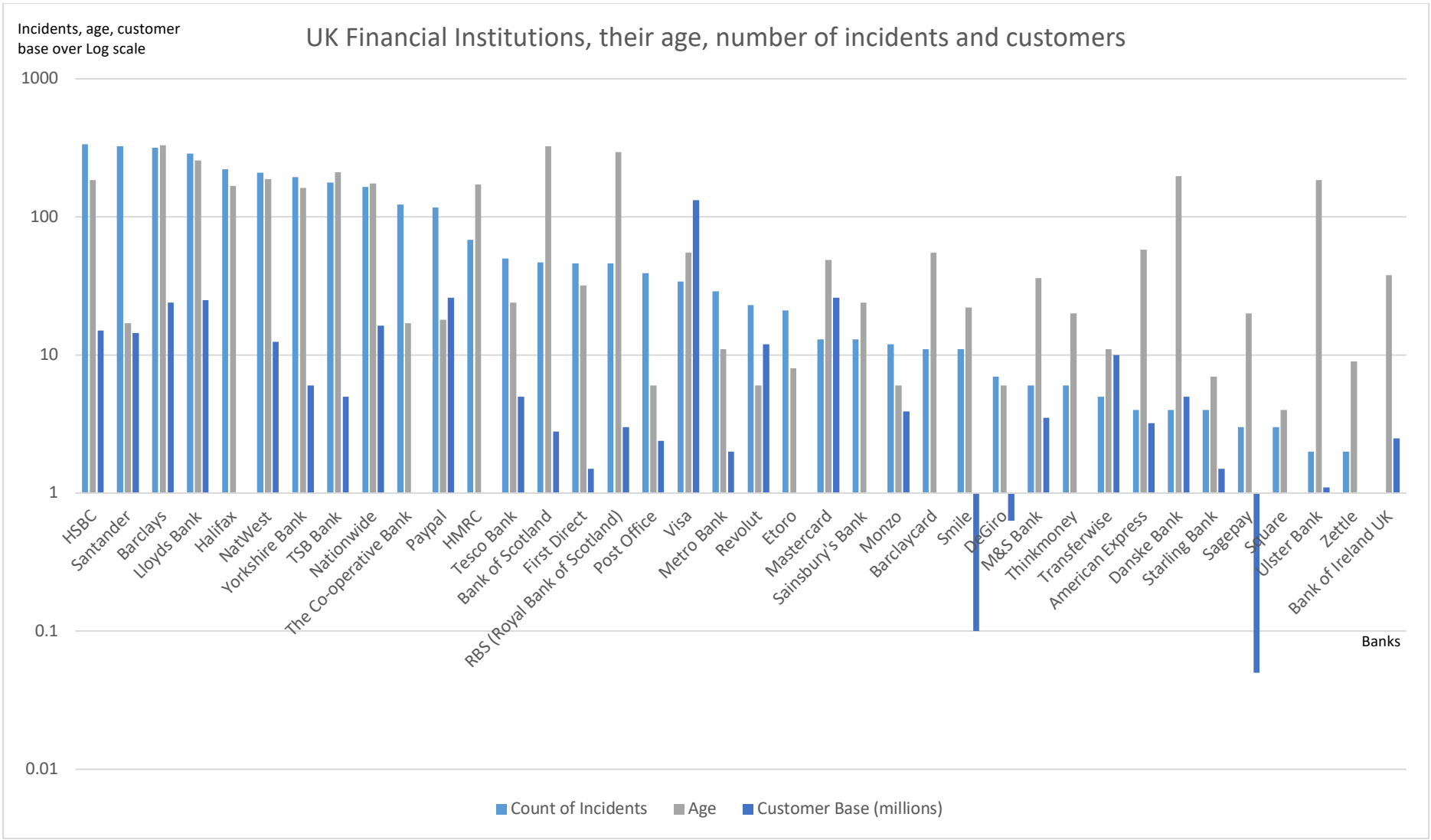


Figure 10 UK Financial Institutions, their age, number of incidents and customers

How incident reports vary by company size and company age as an indication of legacy

The FCA was silent on how it categorises larger and smaller firms in its survey (Financial Conduct Authority, 2018). From Figure 10, it is clear that the older institutions tend to have a higher number of total outages with a few exceptions such as Dankse and Ulster Banks. However, for these exceptions and other institutions, we get additional context when we consider the size of their customer base. Their customer number gives a better view not only of the scale of the technology infrastructure that supports these clients, but also the range of financial products these institutions provide to meet client needs. One could argue about using the age of these institutions is less accurate than using the age of the first computers or automated processes. Another perspective to that argument is the fact that many financial institutions developed processes long before the current evolution of IT systems and some of those processes simply got automated as is. Hence, while considering process management, we see that the age of those institutions is relevant.

Difference in the impact of regulatory programmes that impact the entire sector from ones that affect a part of it

Not all regulatory programmes are equal in scale and impact. We see that when we see the peaks (red rectangle) and troughs (orange rectangle) of incident patterns in Figure 11. They show up in Q4 2017 to Q2 2019. The peak in the red rectangle starts from October 2017 till January 2018 while the trough in orange rectangle is from June 2018 to May 2019. The chart in Figure 12 goes further to focus on the peak outages from October 2017 to January 2018 and the contribution of each Financial institution each month.

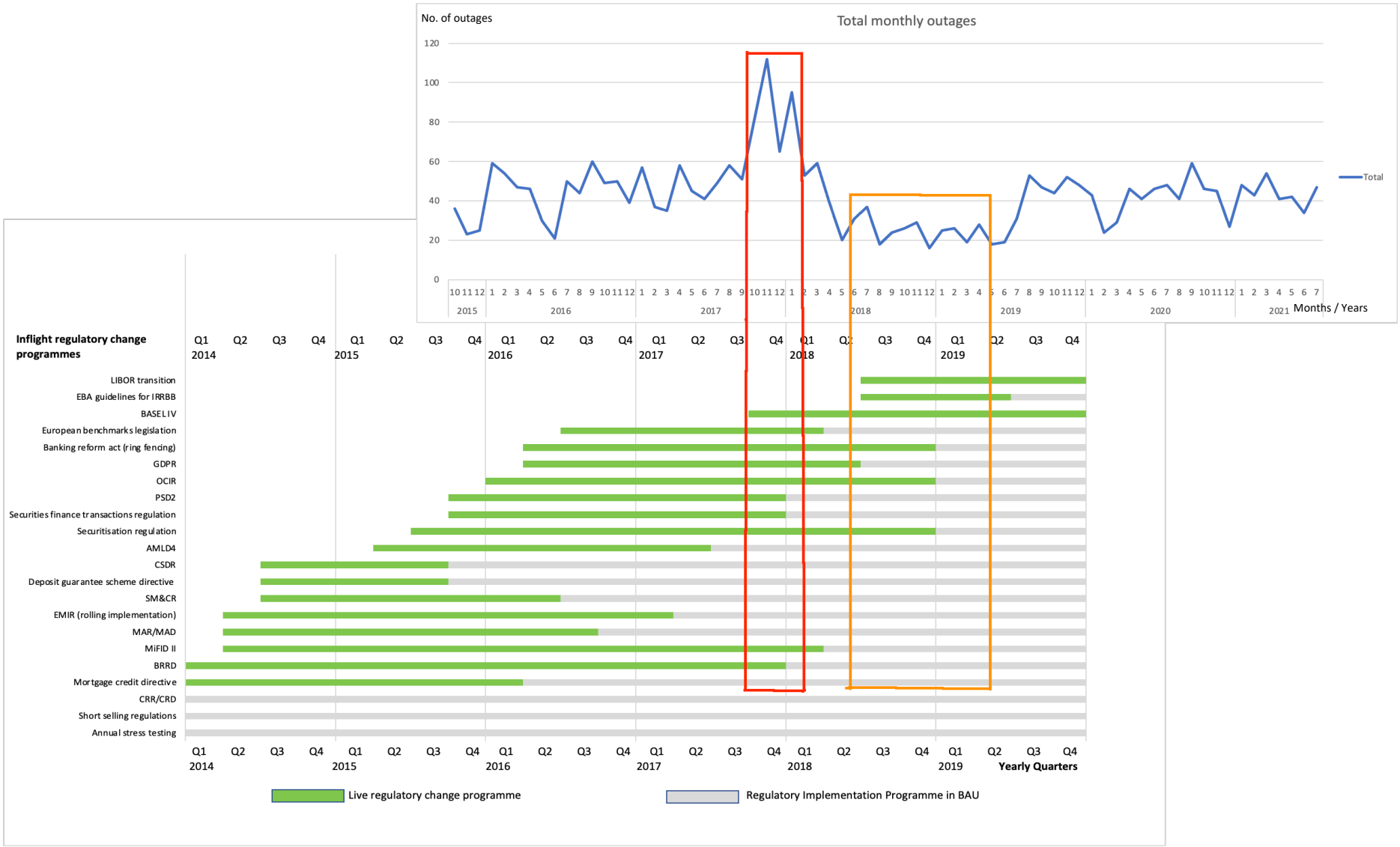


Figure 11 Merging Figure 1 and Figure 3 to align timelines of regulatory programmes and Downdetector incident outage (TheCityUK, 2019, p. 39)

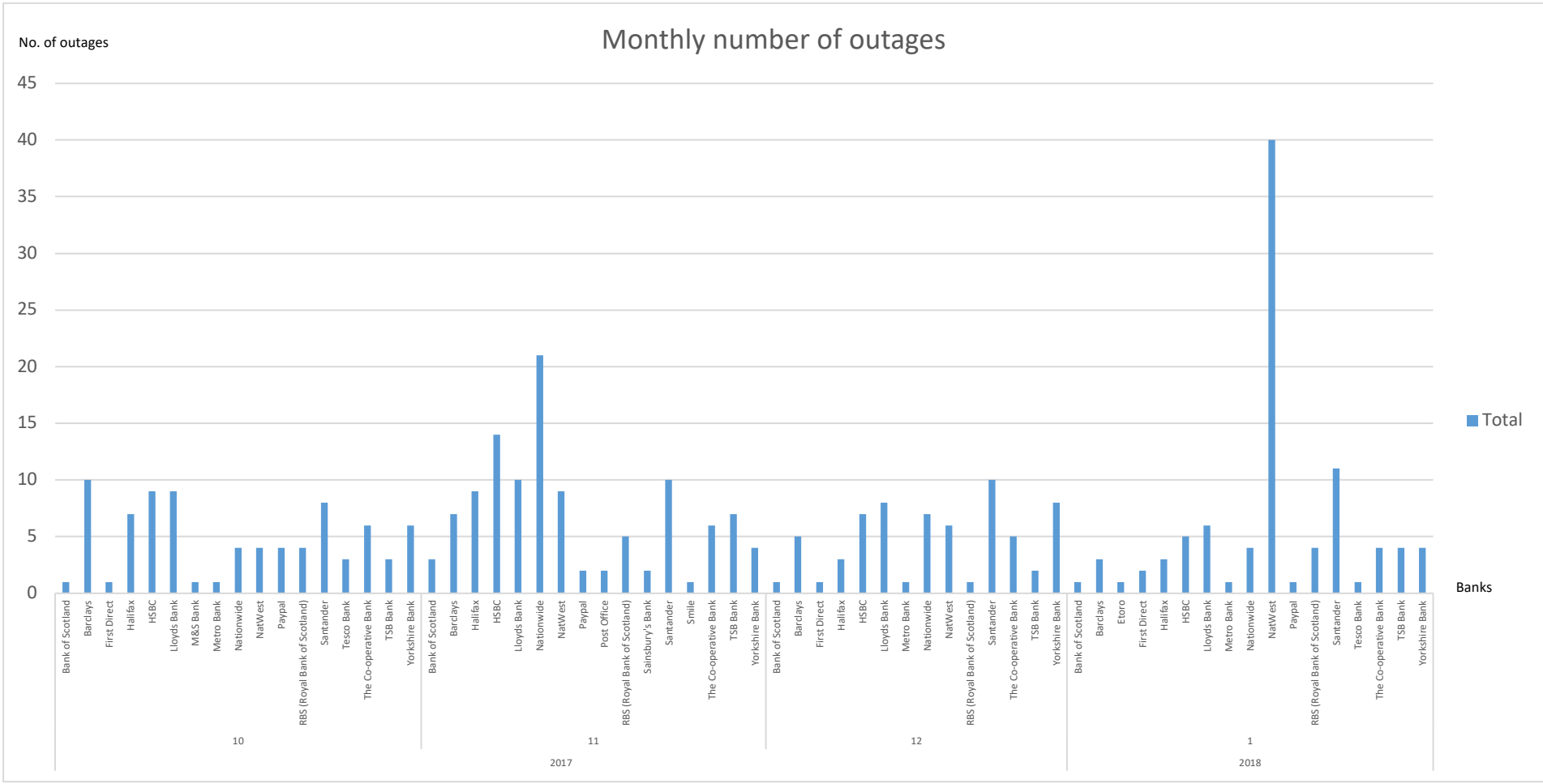


Figure 12 Chart focusing on the peak outages from October 2017 to January 2018

The quarterly number of incidents, number of institutions impacted, and phase of the regulatory programmes have been tabulated in Table 6 for the months around the peak and trough. Table 6 makes it easier to notice the two peak incident quarters are also the quarters with the highest sum of consecutive live programmes getting completed (3+2=5). This suggests that the rush to complete financial services regulatory ahead of their deadlines can increase the rate of technology incidents. The regulatory programmes that fall in this time range include European Benchmarks Regulation, Payment Services Directive 2 (PSD2), Securities Financing Transactions Regulation (SFTR), Markets in Financial Instruments Directive 2 (MiFid II) and Bank Recovery and Resolution Directive (BRRD).

Table 6 Table of Quarterly number of incidents, institutions impacted and phase of regulatory programmes

Yearly Quarter	Quarter Incidents Position	Total Number of incidents	Distinct Number of Institutions	Progs. unstarted	Live Progs. started	Live Progs. ongoing	Live Progs. completed	Previously Completed Progs. (in BAU)
2017 Q2	Pre-Peak	144	16	3	0	9	1	9
2017 Q3	Pre-Peak	158	18	3	0	9	0	10
2017 Q4	Peak	**258**	**20**	**2**	**1**	**6**	**3**	**10**
2018 Q1	Peak / Post-Peak	**207**	**19**	**2**	**0**	**5**	**2**	**13**
2018 Q2	Pre-Trough	90	17	2	0	4	1	15
2018 Q3	Trough	79	19	0	2	4	0	16
2018 Q4	Trough	71	17	0	0	3	3	16
2019 Q1	Trough	70	17	0	0	3	0	19
2019 Q2	Trough	65	21	0	0	2	1	19
2019 Q3	Post-Trough	131	19	0	0	2	0	20
2019 Q4	Post-Trough	144	26	0	0	2	0	20

How GSIBs/GSIFs look individually vs collectively vs entire system

According to the EBA, FSB's 2020 list of GSIBs and the institutions we have data for in this research, we have HSBC, Barclays, and Lloyds as UK banks who are on the list (European Banking Authority, 2020; Financial Stability Board, 2020). We additionally have Nationwide, the Royal Bank of Scotland and Santander UK when we consider the Bank of England's PRA's Other Systemic Important Institutions (O-SIIs) (Prudential Regulation Authority, 2020). Keeping in mind that Natwest and RBS is part of the Natwest group, and Barclaycard is with Barclays, we see that individually and collectively, the 6 institutions take a huge chunk of the incidents from all 43 entities. These institutions are alone responsible for 1697 out of the 2983 incidents (~57%) over the years.

Discussion

The hypothetical questions have been re-listed below as they will be central to this chapter.

H1. Do Concurrent and Consecutive Financial Services Regulatory Programmes impact UK technology systems?
H2. Are Legacy Technology systems less tolerant to several business process changes than modern systems?

For the first question, we have established that some regulatory programmes have more impact on technology systems than others. This confirms what we deduced from existing literature studies. We found out the regulatory programmes end or deadline phase appear to produce the most incidents from technology systems. This suggests that the rush to meet regulatory programme deadlines introduces risk to technology systems. While the Downdetector incident data covers actual customer impact, we need to remember that in certain cases, banks run redundant systems. The implication of such redundant systems is that there are incidents that do not have direct customer impact even if such incidents could be caused by regulatory changes or other reasons. Data from regulatory bodies can provide a more accurate view about these situations besides the fact that such data will not be limited to the retail banking customers. In addition, the data from Downdetector ranged from October 2015 to July 2021 which was insufficient to see what the industry looked like before the 2008 Financial Crisis. With regulatory data from before 2008, we could have clearly compared the stability of the technology systems before and after the re-regulation of the industry.

For the second question, we can conclude that legacy technology systems are less tolerant to business process changes when compared to modern systems. This should be factored in when running regulatory programmes. The research used the age of the financial institutions as an indicator for the probable accumulation of technical debt and consequently, legacy technology systems. The number of customers for these institutions was added to provide a view of the size of these organisations. The data proved that older institutions are more prone to technology incidents than the younger ones. In fact, all GSIBs and most O-SIIs are older banks with among the highest customer bases. We see that both of these groups of financial institutions account for around 57% of all outages from the industry. However, newer institutions, some of which are FinTechs, have significantly fewer technology outages compared to the older ones. According to literature, one of the possible reasons for this is that smaller organisations or FinTech's have fewer regulatory obligations in addition to smaller size.

Conclusion

This research has contributed to major programmes body of knowledge in the following ways. First, this is possibly the first research to use Downdetector as a data source to measure the stability of technology systems. Second, the research has expanded knowledge on programme performance measurement to include system stability of integrated systems and information technology projects within financial services. Third, the research investigates the importance of regulatory changes on financial institutions through event-type analysis. Thus, contributing empirical evidence to our understanding of the interplay of context of projects. Fourth, the research demonstrates that the internal context of financial institutions has an effect on the projects they run.

The research has found that running financial services regulatory programmes impacts the stability of technology systems. This is especially true for legacy technology system architectures that are not as flexible to process changes as modern ones. This conclusion was drawn using secondary outage data from Ookla's Downdetector in the absence of more suitable data from Financial Services regulators. Furthermore, the research found that regulatory programmes tend to impact the stability of technology systems more towards the end phase of such programmes and it is more impactful when the end phases of such programmes align. The Macroprudential view of regulation suggests that both regulators and industry stakeholders should consider how regulatory programmes impact not only single financial services institutions but the industry as a whole. They can be achieved when we are mindful that the financial services industry is a complex system and treat it as such. Hence, while industry regulators try to maintain monetary and fiscal stability, the stability of industry technology systems play a role in the overall stability.

Recommendations

The full potential of this research cannot be realised without the willingness of industry regulators to share data. Actual incident data provided by regulators will reveal areas where customer impact was averted with redundant technology systems. In addition, regulators can provide data for other areas of the financial services industry besides the retail or consumer finance which Downdetector data mostly focuses on. More so, as Scotty Petty from Vodafone UK insists, Downdetector is a great detector but not a flawless detective since it does not tell the full story (Petty, 2020). I recommend that industry regulators become more open to sharing data both for transparency and to facilitate academic research. There are options to anonymise this to cover confidentiality concerns. The technology industry has benefitted from open-source technologies and regulators should adopt this mindset where possible. Furthermore, future researchers should have their institutions register with Ookla's Data for Good initiative. This could potentially provide access to more data than the publicly available Downdetector data used for this research.

Further work

Once data from industry regulators can be obtained, this research can be more useful if financial services organisations are categorised according to the actual regulatory programmes they participate in. This will give more clarity on the actual impact of these regulatory programmes when such data is matched with the incidents or outages that originate from them. In addition, regulatory data can help measure two seasons of the financial services sector: the deregulated season before the 2008 financial crisis and the regulated season after it. The research could be done at a national, continental or global scale.

Instead of using the institution age as an estimate to detect if their systems are legacy or not, actual regulatory or institutional data can be used to arrive at a more accurate assessment of these systems. Once this is obtained, we can normalize the data by finding the rate of technology incidents by year of each systems existence. This will give a fairer assessment of which systems are truly legacy or modern.

While this research has focused on data available from the UK Downdetector arm, it is possible to replicate this research to other countries and compare the outcome. At the time of this research, besides UK instance of Downdetector, there are national websites for Australia, Canada, India, Ireland, New Zealand, South Africa and the United States. This suggests that this UK based research can be extended to 7 other countries.

References

Abusdal, S. & Gjermundnes, R., 2019. *Intelligent Automation in FinTech: An exploratory study of how Norwegian providers of financial technology utilize intelligent automation in light of PSD2,* Bergen: Norwegian School of Economics.

Alfon, I., Argimon, I. & Bascuñana-Ambros, P., 2004. Management views about desired capital: The case of UK banks and building societies. *Journal of Financial Regulation and Compliance,* 12(3), pp. 253-274.

Anagnostopoulos, I., 2018. Fintech and regtech: Impact on regulators and banks. *Journal of Economics and Business,* 100(1), pp. 7-25.

Bank of England, 2021. *Updates to the Bank of England's approach to assessing resolvability - Policy Statement.* [Online]

Available at: https://www.bankofengland.co.uk/paper/2020/updates-to-the-boes-approach-to-assessing-resolvability
[Accessed 1 September 2021].

Barker, S., 2021. *Lloyds Bank, Halifax and Bank of Scotland websites and apps crash in huge IT glitch.* [Online]
Available at: https://www.mirror.co.uk/money/breaking-lloyds-bank-halifax-bank-24566126
[Accessed 25 August 2021].

Bengtsson, E., Holmberg, U. & Jönsson, K., 2013. Identifying systemically important banks in Sweden – what do quantitative indicators tell us?. *Sveriges Riksbank Economic Review,* 2(1), pp. 50-71.

Benner, M. J. & Tushman, M. L., 2003. Exploitation, Exploration, and Process Management: The Productivity Dilemma Revisited. *The Academy of Management Review,* 28(2), pp. 238-256.

Boeker, W. & Huo, Y. P., 1998. Innovation Adoption By Established Firms: Unresolved Issues. *The Journal of High Technology Management Research,* 9(1), pp. 115-130.

Bouyon, S., 2018. *Cost and Value in Banks A model fit for the digital era?,* Brussels: European Credit Research Institute.

Budzier, A. & Flyvbjerg, B., 2011. *Double Whammy – How ICT Projects are Fooled by Ran- domness and Screwed by Political Intent,* Oxford: Saïd Business School, University of Oxford.

Butler, M., 2018. *Cyber and technology resilience in UK financial services.* London, Financial Conduct Authority.

Caruana, J. & Cohen, B. H., 2014. Five questions and six answers about macroprudential policy. *Financial Stability Review - Banque de France*, 1 April, pp. 15-23.

Chakrabarty, K. C., 2014. Framework for the conduct of macroprudential policy in India: experiences and perspectives. *Financial Stability Review - Banque de France*, 1 April, Issue 18, pp. 132-144.

Chapman, R. C., 2012. *Is it possible to establish effective financial services regulatory controls in multi-national enterprises?,* London: Institute of Advanced Legal Studies, University of London.

Cicmil, S., Cooke-Davies, T., Crawford, L. & Richardson, K., 2009. *Exploring the Complexity of Projects: Implications of Complexity Theory for Project Management Practice.* Pennsylvania: Project Management Institute, Inc..

Comella-Dorda, S., Wallnau, K. C., Seacord, R. C. & Robert, J. E., 2000. *A Survey of Legacy System Modernization Approaches.* 1st Edition ed. Pittsburgh: Software Engineering Institute, Carnegie Mellon University.

Darolles, S., 2016. The rise of fintechs and their regulation. *Financial Stability Review - Banque de France*, 1 April, pp. 85-92.

Dombret, A., 2015. *Digital Darwinism and the financial industry – a supervisor's perception.* Oestrich-Winkel, EBS University of Business and Law Symposium.

Dombret, A. R., 2016. Beyond technology – adequate regulation and oversight in the age of fintechs. *Financial Stability Review - Banque de France*, 1 April, pp. 77-83.

Downdetector by Ookla, 2021. *Downdetector Methodology.* [Online]
Available at: https://downdetector.co.uk/methodology/
[Accessed 2021 August 2021].

Ellingsen, C. C., 2018. *The Shock That Doesn't Hurt (yet): A case study of how the second Payment Service Directive is changing the Norwegian banking industry,* Bergen: Norwegian School of Economics.

European Banking Authority, 2017. *Final Report: Guidelines on major incident reporting under Directive (EU) 2015/2366 (PSD2),* Paris: European Banking Authority.

European Banking Authority, 2020. *Global Systemically Important Institutions (G-SIIs).* [Online]
Available at: https://www.eba.europa.eu/risk-analysis-and-data/global-systemically-important-institutions
[Accessed 8 September 2021].

European Commission, 2020. *Anti-money laundering directive IV (AMLD IV) - transposition status.* [Online]
Available at: https://ec.europa.eu/info/publications/anti-money-laundering-directive-4-transposition-status_en
[Accessed 2 September 2021].

Financial Conduct Authority, 2015. *Payment Services Regulations 2017 and Electronic Money Regulations 2011.* [Online]
Available at: https://www.fca.org.uk/firms/payment-services-regulations-e-money-regulations
[Accessed 2 September 2021].

Financial Conduct Authority, 2017. *Information about current account services,* London: Financial Conduct Authority.

Financial Conduct Authority, 2018. *Cyber and Technology Resilience: Themes from cross-sector survey 2017/2018,* London: Financial Conduct Authority.

Financial Stability Board, 2020. *2020 list of global systemically important banks (G-SIBs).* [Online]
Available at: https://www.fsb.org/2020/11/2020-list-of-global-systemically-important-banks-g-sibs/
[Accessed 8 September 2021].

Finder, 2021. *Finder.com.* [Online]
Available at: https://www.finder.com/uk/
[Accessed 12 September 2021].

Flyvbjerg, B., 2014. What You Should Know About Megaprojects and Why: An Overview. *Project Management Journal,* April, 45(2), pp. 6-19.

Flyvbjerg, B., 2017. *Introduction: The Iron Law of Megaproject Management - Oxford Handbooks.* Oxford: Oxford University Press.

Flyvbjerg, B. et al., 2022. The Empirical Reality of IT Project Cost Overruns: Discovering A Power-Law Distribution. *Journal of Management Information Systems,* 39(3), pp. 607-639.

Gill, R., 2011. Why Cloud Computing Matters to Finance. *Strategic Finance,* 92(7), pp. 43-47.

Gu, Y. & Zhu, S., 2015. Assessment of Systemically Important Banks - A Review. *International Journal of Business and Social Science,* 6(9), pp. 1-8.

Hall, K., 2019. *The Convergence of Financial Crime: Guiding Principles for an Effective Integration Initiative,* Ann Arbor: ProQuest LLC.

Harnay, S. & Scialom, L., 2016. The influence of the economic approaches to regulation on banking regulations: a short history of banking regulations. *Cambridge Journal of Economics,* 40(2), p. 401–426.

Hill, R., 2018. *Tech Shutdown Blows: IT chaos cost Brit bank TSB almost £200m.* [Online]
Available at:
https://www.theregister.com/2018/07/27/tsb_reports_loss_100m_it_meltdown_cost_200m/
[Accessed 27 August 2021].

Johnson, N. F., Jefferies, P. & Hui, P. M., 2003. *Financial Market Complexity.* 1st ed. Oxford: Oxford University Press.

Kenton, W., 2021. *MiFID II.* [Online]
Available at: https://www.investopedia.com/terms/m/mifid-ii.asp
[Accessed 31 08 2021].

Knot, K., 2014. Governance of macroprudential policy. *Financial Stability Review - Banque de France*, 1 April, pp. 25-32.

Local Government Association, 2018. *General Data Protection Regulation (GDPR).* [Online]
Available at: https://www.local.gov.uk/our-support/guidance-and-resources/general-data-protection-regulation-gdpr
[Accessed 2 September 2021].

Loesch, S., 2018. *A Guide to Financial Regulation for Fintech Entrepreneurs.* First ed. Chichester: John Wiley & Sons.

LoveMoney, 2020. *Who owns your bank or building society?.* [Online]
Available at: https://www.lovemoney.com/news/15729/who-owns-your-bank-or-building-society
[Accessed 25 August 2021].

M&S Bank, 2021. *M&S Bank Financial Services Compensation Scheme (FSCS).* [Online]
Available at: https://bank.marksandspencer.com/about-us/fscs-protection/
[Accessed 28 August 2021].

Maylor, H., Blackmon, K. & Huemann, M., 2017. *Researching Business and Management.* 2nd ed. London: Palgrave.

Munbodh, E., 2018. *Barclays customers told they won't have access to online banking this weekend as part of 'maintenance' plans.* [Online]
Available at: https://www.mirror.co.uk/money/barclays-customers-told-lose-access-12661266
[Accessed 9 September 2021].

Petty, S., 2020. *Why Downdetector is not the perfect detective.* [Online]
Available at: https://newscentre.vodafone.co.uk/viewpoint/downdetector-not-the-full-picture-outages/
[Accessed 13 September 2021].

Pierri, N. & Timmer, Y., 2021. The importance of technology in banking during a crisis. *European Systemic Risk Board: Working Paper Series,* Issue 117, pp. 1-58.

Prudential Regulation Authority, 2020. [Online]
Available at: https://www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/crd-iv/2020-list-of-uk-firms-designated-as-osiis.pdf
[Accessed 8 September 2021].

Raghavan, K., 2007. A survey of corporate governance and overlapping regulations in banking. *International Journal of Disclosure and Governance,* 4(3), p. 181–194.

Robinson, L., 2011. The Cloud: Bringing Permanent Changes to Business. *Financial Executive,* 27(10), pp. 71-72.

Ronzon, T., 2016. Software Retrofit in High-Availability Systems: When Uptime Matters.. *IEEE Software,* 33(2), pp. 11-17.

Sabherwal, R., Jeyaraj, A. & Chowa, C., 2006. Information System Success: Individual and Organizational Determinants. *Management Science,* 52(12), p. 1849–1864.

Statista, 2021. *Statista.* [Online]
Available at: www.statista.com
[Accessed 12 September 2021].

Taleb, N. N., 2010. *The Black Swan - The Impact of the Highly Improbable.* 2nd ed. London: Penguin Random House.

The Guardian, 2021. *Online banking and gaming services hit by internet outage.* [Online]
Available at: https://www.theguardian.com/technology/2021/jul/22/online-banking-and-gaming-services-hit-by-internet-outage
[Accessed 23 August 2021].

TheCityUK, 2019. *Operational Resilience in Financial Services - Time to Act,* London: TheCityUK Research.

Treynor, B., Dahlin, M., Rau, V. & Beyer, B., 2017. The Calculus of Service Availability. *Communications of the ACM,* 60(9), pp. 42-47.

Tushman, M. L. & Anderson, P., 1986. Technological Discontinuities and Organizational Environments. *Administrative Science Quarterly,* 31(3), pp. 439-465.

Twitter, 2021. *Twitter Page Conversation of HSBC UK and FirstDirect Customers.* [Online]
Available at: https://twitter.com/colmlonergan/status/1420772991575670784
[Accessed 28 August 2021].

UKFinance, 2018. *UK Card Payments 2018,* London: UK Finance.

Wali, A. F., 2016. *A Comparative Consumer Study of Firms' CRM Practices and Marketing Effectiveness in the Mobile Telecommunications Sectors of Nigeria and the UK,* Huddersfield: University of Huddersfield Repository.

Wright, M., 2020. *How safe are your savings?.* [Online]
Available at: https://www.moneysupermarket.com/money-made-easy/who-owns-who/
[Accessed 26 August 2021].