PARETO

Undergraduate Journal of New Economists

University of Toronto Mississauga

Title: The Impact of Open Banking on Economic and Financial Crime

Author: Michael Kemp

Source: *PARETO: Undergraduate Journal of New Economists*, Vol. 2, Winter 2024

Published By: Department of Economics, University of Toronto Mississauga

Stable URL: https://doi.org/10.33137/pugj.v2i1.44733

Economics
UNIVERSITY OF TORONTO
MISSISSAUGA

The Impact of Open Banking on Economic and Financial Crime

By Michael Kemp

This paper attempts to answer the research question: How does Open Banking impact economic and financial crime? To answer this, panel data on crimes committed in the United Kingdom that span a ten-year period was collected. Using the definition of economic and financial crime most common in the existing literature, data were filtered to include only relevant crimes. Using the synthetic control method to analyze Open Banking as a policy effect, this paper finds evidence that Open Banking leads to increased levels of fraud and blackmail.

***Keywords**: Open Banking, FinTech, Marketplace lending, Financial Crime, Economic Crime, Business and Securities Law, Synthetic Controls*

***DOI**: https://doi.org/10.33137/pugj.v2i1.44733*

I. Introduction

Technology is transforming the financial industry and altering the threats it faces. The 2008 financial crisis created a distrust in traditional financial institutions [Buckley et al. (2016)]. This distrust primed the financial industry for disruption via new innovators and gave rise to fintechs, a class of firms that use technology to improve existing financial services [Suryono et al. (2020)]. In the decade following the financial crisis, thousands of fintechs were founded and tens of billions of dollars were invested into the fintech industry. The rise of fintechs also challenged the existing banking structure and generated new models of banking such as Open Banking. Open Banking, which allows consumers to share their data stored at traditional financial institutions with FinTechs, is experiencing rapid growth alongside the fintech industry. In combination with Open Banking, FinTechs perform a variety of services such as investing, fraud prevention, etc., allowing individuals to derive more utility from their banking data. The United Kingdom, the world's leading adopter of Open Banking policies, has over 6 million active Open Banking users which represents roughly ten percent of the country's population [OpenBanking.org (2022)].

Despite the rapid adoption of Open Banking policies around the globe, research on the topic is scant. This is concerning, especially in the area of economic and financial crime which has received little to no attention from researchers. Cybercrime, including: fraud, identity theft, and other types of economic and financial crimes impacting consumers, has reached a record high [FTC (2022)]. This type of crime is increasingly being perpetrated by external actors such as hackers and organized crime networks, which are immune to traditional fraud prevention tools [Price-Waterhouse-Cooper (2022)]. Given that Open Banking has greatly increased the movement of sensitive financial data, a perfect storm of potential vulnerabilities has been forming. It is crucial that governments understand the implications of Open Banking before implementing policies that may have greater consequences than benefits.

This paper seeks to clarify the relationship between Open Banking and financial crime. The impact of Open Banking on financial crime has been investigated before but research has only arrived at ambiguous theoretical predictions. This warrants further empirical analysis to understand the magnitude of the problem. Analysis in this paper will focus on the United Kingdom, the worlds leading adopter of Open Banking policies.

II. Literature Review

Given the proliferation of Open Banking only in the past several years, the literature on the topic is recent and limited. Empirical studies linking Open Banking policies with economic and financial crime are generally non-existent in the literature. However drawing on the limited publications surrounding Open Banking and financial crime can still help inform this paper's analysis. Gozman, Hedman, and Sylvest utilized the recursive identification of patterns method to identify risks and benefits presented by Open Banking [Gozman et al. (2018)]. Following a collective case study methodology, these authors drew on primary interview data and secondary quantitative data from five financial institutions impacted by Open Banking to conduct their analysis. Their analysis focused on a theoretical evaluation of the possible outcomes of Open Banking policies on fraud and other related crimes. Similarly, the work of Brodsky and Oakes relied on the literature surrounding application programming interfaces (APIs), programs that allow for the sharing of data between systems, to facilitate their discussion of the potential impact of Open Banking on financial crime [Brodsky and Oakes (2017)]. Their paper focused on the implications that Open Banking policies have on data sharing within the European financial industry. Open Banking had just been implemented when both papers were written and relevant data was limited. Both papers are purposely ambiguous about the direction of Open Banking's impact on economic and financial crime due to their qualitative nature. By examining the possible contingencies of Open Banking, both papers give essential insights into the possible theoretical outcomes of policy decisions.

Other attempts have been made to uncover the links between Open Banking and financial crime. Achim, Borlea, and Vãidean conducted an empirical analysis of the effect of technology on economic and financial crime [Monica-Violeta et al. (2021)]. Their paper analyzed economic and financial crime at a global level by utilizing data from 185 countries. To measure economic and financial crime, they aggregate index measures of corruption, the shadow economy, and money laundering to create the economic and financial crime index. This work serves as one of the few quantitative studies on financial crime and technology related policy changes.

This paper builds on the existing literature by conducting a novel empirical analysis measuring the impact of Open Banking on economic and financial crime. By taking a structural approach, this paper is able to better measure the magnitude of the causal effect of Open Banking policies on economic and financial crime. Namely, this is achieved using the synthetic control methodology which, allows us to see the impact of Open Banking at the country-wide level; and therefore analyze Open Banking as a country-wide policy rather than at the firm level.

Additionally, this paper focuses on the impact of Open Banking using a novel measure of economic and financial crime. This paper utilizes exact counts of consumer fraud, identity theft, and other crimes that fall under the definition of economic and financial crime to conduct its analysis. The advantage of this approach is that the effect of Open Banking on specific types of crimes can directly be measured. Taking an aggregate approach does not allow for distinction between individual crimes. This work contributes to the literature on economic and financial crime by allowing for the impact of Open Banking to be analyzed at the level of each individual crime as well as an aggregate level.

III. Conceptual Framework

This section outlines the theoretical strategy employed in this paper to analyze the effect of Open Banking on economic and financial crime.[1] To allow for the analysis of Open Banking's effect on specific types of crime, aggregate measures of crime used in other studies cannot be utilized. Instead, this paper utilizes exact counts of specific types of economic and financial crime. This allows for the effects of Open Banking to be analyzed in terms of each individual type of crime. Analysis focuses on a single country that has implemented Open Banking. How crime is defined, measured, and prosecuted differs drastically by country. While aggregate levels of crime can be accurately compared across countries, types of individual financial crime will vary drastically by country and not be directly comparable [Monica-Violeta and Sorin (2020)]. Therefore, to consistently measure the effect of Open Banking across different types of crime, it is best to narrow the scope of analysis to a single country. Given Open Banking is a novel concept, it exists in only a select number of countries. Of these select countries, only the United Kingdom has made Open Banking formal and compulsory via national legislation.

Open Banking came into law in the UK in the first quarter of 2018 [OpenBanking.org (2022)]. While other nations such as Japan and India have encouraged financial institutions to implement Open Banking, their lack of formal legislation has resulted in an inconsistency in the implementation of Open Banking across their financial industries. This inconsistency in implementation means the impact of Open Banking cannot be properly measured at a national level as segments of the population are unaffected. Thus, to best measure the impact of Open Banking, this paper will narrow its focus to the United Kingdom. The United Kingdom's national Open Banking legislation, coupled with the fact it is the world's leading adopter of Open Banking, make it an ideal case study. This paper takes an econometric policy analysis approach utilizing panel data techniques. Demographic and economic factors, the main drivers of crime, such as unemployment rates, and population are accounted for.

The effect of Open Banking on economic and financial crime is ambiguous. The two most prevalent theories on how Open Banking may impact crime provides for both increased and decreased crime. There are a number of channels through which Open Banking may affect crime. This paper focuses on the most prevalent channel within the literature, data transfer.

The first theory within the literature is that Open Banking will exacerbate economic and financial crime, specifically fraud connected to an individual's data [Gozman et al. (2018)]. It is argued that the increased flow of sensitive financial data throughout the financial system will lead to more points of potential vulnerability. Individual's data, which has traditionally been under the stewardship of financial institutions, is now flowing to third parties. An argument can

[1] There is no single definition of economic and financial crime. Economic and financial crime refers to a broad umbrella of economically motivated crimes such as credit card fraud, insider trading, drug trafficking, etc. Using the most common definitions in international law and the existing literature on the topic, this paper defines economic and financial crime as the taking of money, property, or any other crime where economic gain is the primary motive

be made that this provides greater vulnerability for fraudsters and hackers [Brodsky and Oakes (2017)]. Literature on the topic has shown that more third party entities can lead to weak links that may expose an individual's data to risks [Kunreuther and Heal (2003)]. Additionally, while banks have infrastructure such as "know-your-customer" procedures that validate the identity of customers and other security measures, it is possible that fintechs may not have the same security and robustness against potential data breaches [Gozman et al. (2018)]. Thus, it is possible that Open Banking, which greatly increases the flow of financial data between entities, may exacerbate fraud.

In contrast, there exists another stream of literature that suggests data sharing will reduce breaches. Various authors have shown that systems structured as associations of clubs reduce the risk for potential hidden action [Anderson and Moore (2006)], [Zhang et al. (2024)]. When information is shared between more entities, it goes through tightened checks, auditing, and security systems, making it difficult for potential breaches to occur. Financial institutions and fintechs, which have become an association of clubs due to Open banking, will have more measures on aggregate in place to protect consumer data. Thus, it is possible that Open Banking, which creates an association between financial institutions and fintechs, could reduce fraud. Overall the effect of Open Banking is somewhat ambiguous.

IV. Data

This paper draws on two primary sources of data to create a novel panel data set. The first data source is the 2022 Police Recorded Crime Open Data Tables from the Home Office of the United Kingdom. The 2022 Police Recorded Crime Data Tables cover crime statistics within England and Wales spaning the years 2012 to 2022. The principal purpose of this data set is to quantify the number of each type of crime in England and Wales. The data set includes exact counts of every defined category of crime in England and Wales, by police jurisdiction, by quarter, and by year. The data shows how each type of crime is trending over time and facilitates the analysis of Open Banking in relation to individual crimes. The key variables from this data set are Offense Code, Offense Description, and Number of Crimes. One limitation of the 2022 Police Recorded Crime Open Data tables is that crime numbers for Scotland and Northern Ireland are not included in the data. Detailed crime statistics for Scotland and Northern Ireland are recorded separately and are not readily available to the public. Given England and Wales make up the majority of the population of the United Kingdom and have both been identically affected by the national Open Banking legislation, the data is more than sufficient to facilitate an analysis of Open Banking.

The second primary data source for this paper comes from the OECD economic and demographic statistics for the United Kingdom. The data set is quarterly panel data that spans from 2012 to 2022. This data provides key predictors of economic and financial crime. Key variables taken from the data set are unemployment rates, GDP per capita, and population. A limitation of this data is that it is for the entire United Kingdom and not just England and Wales. Most data in the United Kingdom is reported on aggregate and not just for England and Wales. To get consistent measures of all the key demographic and economic variables needed for the analysis of Open Banking, aggregate United Kingdom levels were included for consistency. England and Wales comprise 90 percent of the United Kingdom's population. Their economic and demographic trends are virtually identical to the United Kingdom as a whole. Thus, United Kingdom demographic and economic statistics are adequate as they accurately reflect the same statistics in England and Wales.

The data set used in this paper is constructed by merging the two primary data sources using a common year and quarter variable. All crimes that do not meet the definition of economic and financial crime were then dropped from the data set. Summary statistics for key variables of the data set are found in appendix table A1. GDP Per Capita and Population variables are measured in thousands. The Unemployment variable is the unemployment rate in percent. The most important of these summary statistics surround the Number Of Crimes variable. This variable measuring the number of crimes uses the count of a specific crime in a given year and quarter. As seen in table A1, there is great variation between the Number of Crimes with the minimum being 21 and the maximum being 224,284. This indicates that some crimes are very small in total count while others are far more common. There are 1,440 total observations, corresponding to the 40 periods of data over 36 categories of economic and financial crime.[2]

To facilitate the use of a synthetic control method, discussed in the next section, three unique variables were created. Crime Per Capita was created by dividing the Number of Crimes variable by the Population variable. This indicates crime levels relative to the population of the United Kingdom. The Crime GDP Per Capita Ratio was created by dividing the Number of Crimes variable by the GDP Per Capita variable. This provides a ratio showing the relationship between crime and GDP per capita levels. The Crime Unemployment Ratio was created by dividing the Number of Crimes variable by the Unemployment rate variable. These three variables, while different, are all relative measures of crime within the United Kingdom. The synthetic control method requires predictors of the variable of interest, in the case of this paper, the Number of Crimes variable [Abadie (2021)]. As noted in the existing literature, different measures of the target outcomes are suitable auxiliary covariates to use as predictors in the synthetic control method [Shi et al. (2021)].

A. Empirical Strategy

The primary empirical strategy used in this paper is the synthetic control method. The synthetic control method is a frontier technique used to measure the impact of aggregate interventions, such as national policies [Abadie (2021)]. In the case of this paper, the aggregate entity is the United Kingdom and the affected units are the individual economic and financial crimes within the United Kingdom. The goal of the synthetic control method in this paper is to measure the impact of Open Banking on the number of crimes.

The synthetic control method works by creating a synthetic version of a treated unit from a weighted average of similar untreated donor pool units [Abadie (2021)]. The method uses an algorithm that minimizes the difference between the treated unit and the synthetic unit over the pre-treatment period while simultaneously predicting how it would have trended post-treatment [Abadie (2021)]. The treatment date for this analysis will be defined as having been during quarter one of 2018 when Open Banking came into law in the United Kingdom [OpenBanking.org (2022)]. A key assumption required for identification in the synthetic control model is that the

[2] See table A2 for a complete list of all economic and financial crimes

donor pool units must be similar in nature to the treated units. For this reason, the data set used in the analysis was restricted to economic and financial crime. These types of crimes, are similar in motive and nature and will best allow for identification. While expanding the donor pool to include a greater variety of crimes would give a larger donor pool, it would threaten identification by including crimes that are not similar in nature or motive to the treated crimes impacted by Open Banking [Shi et al. (2021)].

In this paper, any economic or financial crime likely to be impacted by Open Banking is considered to have been treated. As discussed, these are crimes that involve an individual's financial data. The most common crimes in this category are consumer fraud, business fraud, and blackmail. Consumer and business fraud are measured in the United Kingdom via three national agencies; Action Fraud, CIFAS, and UK Finance. Action Fraud is based on police-measured counts of fraud, CIFAS is designed by conglomerate of businesses that measure consumer and business fraud among their members, and UK Finance is the government's official measure of fraud. These three agencies, which all measure fraud slightly differently, give a good indicator of the level of consumer and business fraud in the United Kingdom at any given time. Thus, the four treated units in this analysis are Action Fraud, CIFAS, UK Finance, and Blackmail. All other economic and financial crimes, listed in table A2, are considered untreated and make up the donor pool.

Auxiliary covariates, called predictors, are time-specific vectors of factors shared across different units. They are used to assist the model in choosing the optimal weights of donor pool units to construct a synthetic unit [Shi et al. (2021)]. There are two types of suitable auxiliary covariates. The first are covariates related to the variable of interest. [Abadie (2021)], the creator of the method, provides the example of beer consumption as a predictor for smoking levels within U.S states. The second type of suitable auxiliary covariate is derived from different measurements of the variable of interest. This paper utilizes the second type of auxiliary covariates as they are just as accurate and much easier to implement than the first type [Shi et al. (2021)]. As outlined in the data section of the paper, the Crime Per Capita, Crime GDP Per Capita Ratio and the Crime Unemployment Ratio are all different measures of the Number of Crimes variable. This paper utilizes these three variables as auxiliary covariates when creating synthetic crimes.

Using the defined auxiliary covariates and donor pool of untreated crimes, this paper will run the synthetic control method on Action Fraud, CIFAS, UK Finance, and Blackmail. Synthetic versions of each of these crimes will be created. By plotting the differences between the real and synthetic versions of each crime this paper will measure the impact of Open Banking on financial crime.

B. Formal Specification of the Synthetic Control Model

Using the methodology of [Abadie (2021)], this paper formalizes the synthetic control method with Open Banking. For each type of crime i, and time t we observe the outcome of our variable of interest, $Crime_{it}$. Assume that $i = 1$ is a treated crime affected by Open Banking and $I + 1$ is a collection of untreated donor pool crimes. For each crime, i, and time, t, this paper defines $Crime_{OB}$ it as the potential response of a crime under Open Banking policies. For each crime, i, and time, t, this paper defines CrimeNit as the potential response of a crime in the absence of Open Banking policies. Therefore, the effect of Open Banking for an affected unit in period t is:

$$\tau_{1t} = Crime_{it}^{OB} - Crime_{it}^{N} \tag{1}$$

Synthetic control methods aim to produce an estimate of $Crime_{1t}^{N}$, the value of the variable of interest that would have been observed for the affected unit in absence of an intervention, Open Banking in this case [Abadie (2021)]. Given a vector of our optional weights of $I+1$ donor pool crimes, $W = (w_2, ..., w_{i+1})$, the synthetic control estimates of τ_{1t} and $Crime_{it}^{N}$ in this paper are:

$$Cri\hat{m}e_{1t}^{N} = \sum_{i=2}^{I+1} Crime_{it} \tag{2}$$

and

$$\hat{\tau_{1t}} = Crime_{1t} - Cri\hat{m}e_{1t}^{N} \tag{3}$$

Where individual weights must be non-negative and the total weighting must sum to one.

C. *Why Synthetic Control?*

The synthetic control method was utilized over other traditional policy analysis techniques such as the difference-in-differences method due to a lack of a comparable control group. How crime is measured and defined varies greatly by country. Thus, a specific type of crime will generally not exhibit the same trend across countries. This problem is exacerbated by the fact that crime numbers are heavily influenced by country-specific events. As seen in figure 1 and figure 2, crime numbers for treated and untreated crimes in the United Kingdom experienced several sharp spikes:

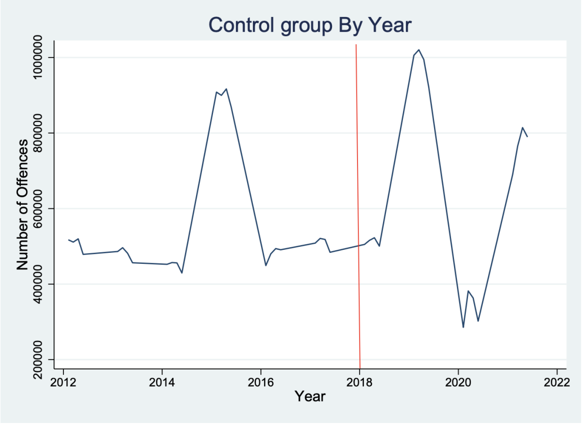


Figure 1. Donor Pool Crimes by Year

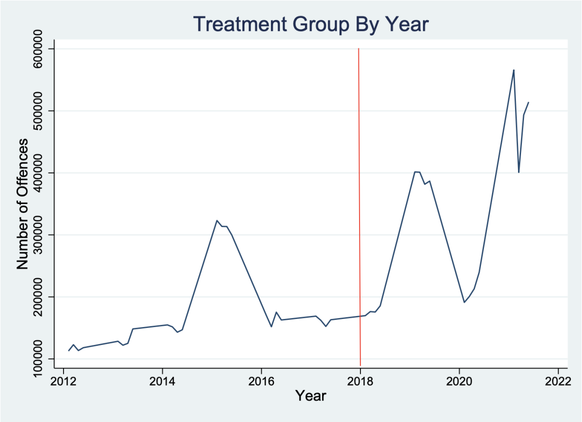


Figure 2. Treated Crimes by Year

These spikes correspond to a crackdown by the government on white collar crime in 2015 and cuts to civil service funding in the years leading up to 2019. These country-specific events, coupled with the inherent difference in how crime is measured and defined across countries, make it impossible to find a comparable country to satisfy the parallel trends assumption needed for other panel data methodologies.

Thus, given the lack of an appropriate control group, the synthetic control method was the best possible methodology. By creating synthetic controls out of different untreated crimes in the United Kingdom which follow the same country-specific trends (figure 2 and figure 3), a policy analysis of Open Banking was logically sound and practical to implement.

V. Results

The main results of this paper's synthetic control analysis were created using the three predictor variables as they improved the accuracy of the synthetic control for some of the treated crimes. The time periods with corresponding with the COVID-19 pandemic (2020 Q2 onward), were dropped from the sample. As seen in table 1 below, dropping COVID-19 had no impact on any of the synthetic controls and did not change the pre-treatment mean differences.[3] Note that Open Banking was implemented in the United Kingdom in quarter one of 2018.

Table 1—Overall Results: Mean Differences

	Main Specification		
Crime Recorded	Pre-Treatment	Post-Treatment	Pre-Treatment Avg.
Action Fraud	-284.6	60162	64560
Blackmail	-106.2	3515	1501
CIFAS	-1700.9	27981	77680
UK Finance	-32.2	27184	28133
	Covid Dropped from Specification		
Crime Recorded	Pre-Treatment	Post-Treatment	Pre-Treatment Avg.
Action Fraud	-284.6	36574	64560
Blackmail	-106.2	1822	1501
CIFAS	-1700.9	14813	77680
UK Finance	-32.2	4586	28133

Figure 3 below shows Action Fraud plotted against Synthetic Action Fraud over time. Synthetic Action Fraud did an excellent job of matching the pre-treatment trend of the real Action Fraud. Coupled with the fact that the average pre-treatment mean difference was -284.62, which is close to zero, the results of the synthetic control method on Action Fraud can be taken as accurate.[4]. The post-treatment impact of Open Banking on Action Fraud was a magnitude increase of an average of 36,573 crimes. This constitutes a significant 56.70 percent increase compared to the pre-treatment average number of crimes. Synthetic action fraud was made up of a combination of 56.8 percent 'Shoplifting' and 43.2 percent 'Making off Without Payment'. Dropping the predictors and the time periods that included Covid did not impact the weighting,

[3] Action fraud weights did not change when the predictors or covid were dropped from the main specification

[4] See appendix figure A1 for a robustness visualization

indicating the initial results are relatively robust. Results with and without predictors for Action Fraud are shown in appendix figure A2. These results can be taken as an early indication that Open Banking has impacted consumer and business fraud.

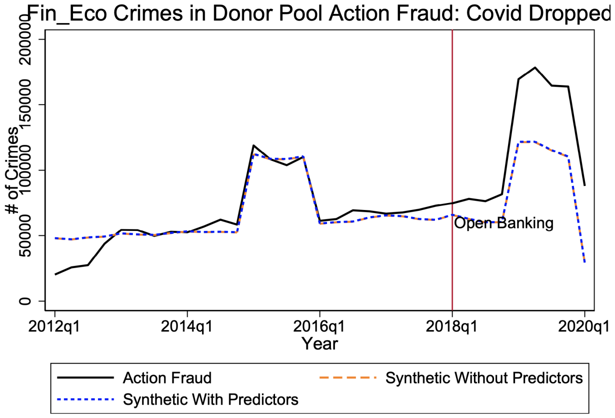


Figure 3. Action Fraud Synthetic Covid Dropped

Similar to Action Fraud, the results of the synthetic control being run on Blackmail are accurate. Figure 4 below shows that Synthetic Blackmail closely matched Blackmail during the pre-treatment period. The average pre-treatment mean difference between Synthetic Blackmail and Blackmail was -106.24. The pre-treatment trend is essentially zero. Results with and without predictors for Blackmail are shown in appendix figure A3. The post-treatment impact of Open Banking on Blackmail was an increase of an average of 1,822 crimes. This is a significant increase of 121.34 percent compared to the pre-treatment average number of crimes of 1501. Like Action Fraud, dropping predictors and the time periods corresponding to COVID-19 did not impact the weighting of the synthetic control. It can be interpreted that Open Banking has resulted in increased levels of Blackmail.

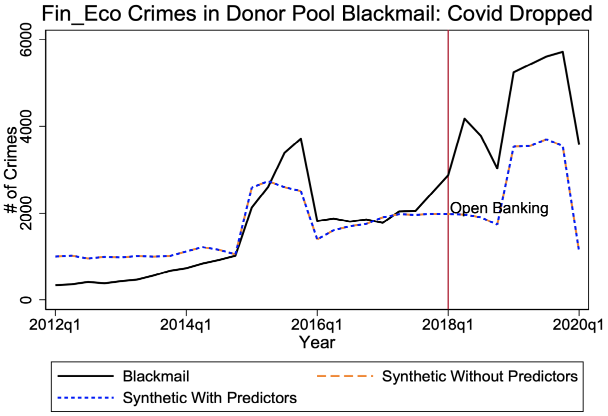


Figure 4. Blackmail Synthetic Covid Dropped

In contrast to Action Fraud and Blackmail, the results of the synthetic control run on CIFAS, while relevant, should be taken with some skepticism. As seen in figure 5 below, from a visual perspective Synthetic CIFAS does a good job of matching CIFAS. Although, given the pre-treatment average difference is -1700.91, it can be seen that parallel trends were not as closely satisfied as with Action Fraud. This synthetic control has difficulty modelling the pre-treatment trend. It is also important to note, that CIFAS has the highest average level of pre-treatment crimes at 77,680. This is likely the reason the pre-treatment difference is higher in magnitude. The post-treatment average increase in crimes for CIFAS was an increase of 19.07 percent compared to the pre-treatment average. The Synthetic version of CIFAS is virtually identical with and without predictors. Results with and without predictors for CIFAS are shown in appendix figure A4. The analysis of CIFAS suggests, less strongly than the results of Action Fraud and Blackmail, that Open Banking leads to an increase in business and consumer fraud.

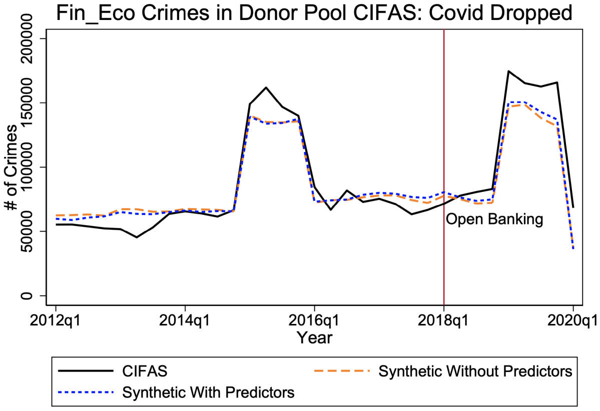


Figure 5. CIFAS Synthetic Covid Dropped

Lastly, the results of the synthetic control method used on UK Finance, visualized in figure 6 below, are quite interesting. With a mean pre-treatment difference of -32.21, Synthetic UK Finance is the most accurate synthetic control in this paper. However, the post-treatment average difference is a magnitude increase of only 4,585.91 crimes. This constitutes a modest 7.89 percent increase from the pre-treatment average. In terms of robustness, it can be seen that the results of UK Finance are not as robust as the other treated units. As seen in appendix figure A5, Synthetic UK Finance without predictors does a similar job of predicting the pre-treatment trend but indicates a negligible increase in the magnitude of crimes post-treatment. Thus, given the lack of robustness and the modest magnitude increase, the interpretation of the results of UK Finance should be that of Open Banking having little affect on consumer and business fraud.

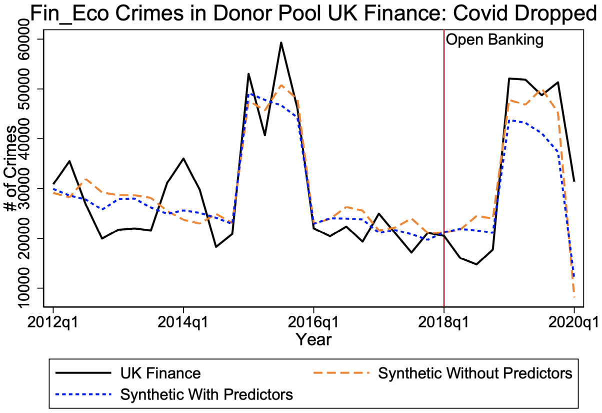


Figure 6. UK Finance Synthetic Covid Dropped

VI. Robustness

As mentioned in the main results, none of the treated units were impacted by dropping the periods corresponding with COVID-19. Action Fraud, Blackmail, and CIFAS were unaffected by the dropping of predictor variables. The results of UK Finance were significantly impacted when the predictor variables were dropped, indicating its results are not as robust. Given the difficulty of obtaining p-values and standard errors for inference when using the synthetic control method, this paper presents a number of additional robustness tests and alternate specifications. The works of [Abadie (2021)] and [Shi et al. (2021)] provide a number of different robustness tests for the synthetic control method.

Back dating is the process of changing the treatment date in the synthetic control algorithm to an earlier date than the actual intervention date [Abadie (2021)]. Back dating the treatment effect shows robustness if the weights that make up the synthetic control are unaffected by the back dating. Back dating resulted in no changes to the weights of the synthetic versions of any of the treated units. Visualized in appendix figure A1, it can be seen that backdated synthetic Action Fraud is identical to regular Synthetic Action Fraud. This is the same for all other synthetic controls, where the weights of action fraud have not changed. These results indicate that the treatment, Open Banking, is being properly captured by the model. Had backdating caused a significant change in the synthetic controls it would have been an indication of a lack of robustness in the model.

'Leaving out' is considered another valuable robustness test. The leaving out test is when one, or several of the weights that make up a synthetic version of a unit are dropped from the data set [Shi et al. (2021)]. The synthetic control estimation is run again to see how well the trend can be matched. If the differences between the actual unit and the synthetic unit have varied only slightly it shows the results are robust. Leaving crimes out of each synthetic control's donor pool resulted in no significant changes to any of the synthetic versions of the treated units. Synthetic control Action Fraud is made up of "Shoplifting" and "Making off Without Payment". As seen in figure 7 below, when these two crimes are dropped from the donor pool, the synthetic control method still does an almost identical job of matching the trends. This indicates that the donor pool of crimes is robust as other types of less optimal crimes can construct a synthetic crime.

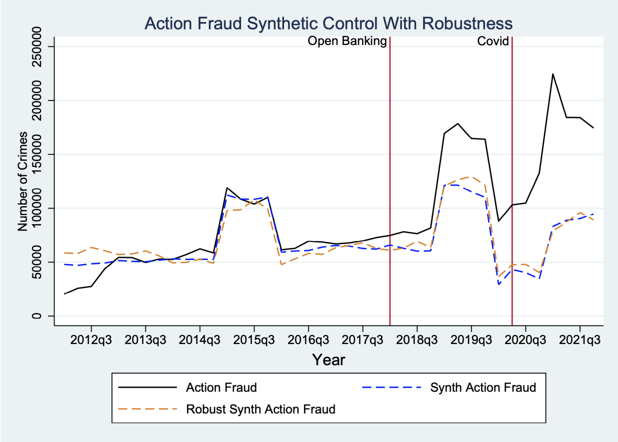
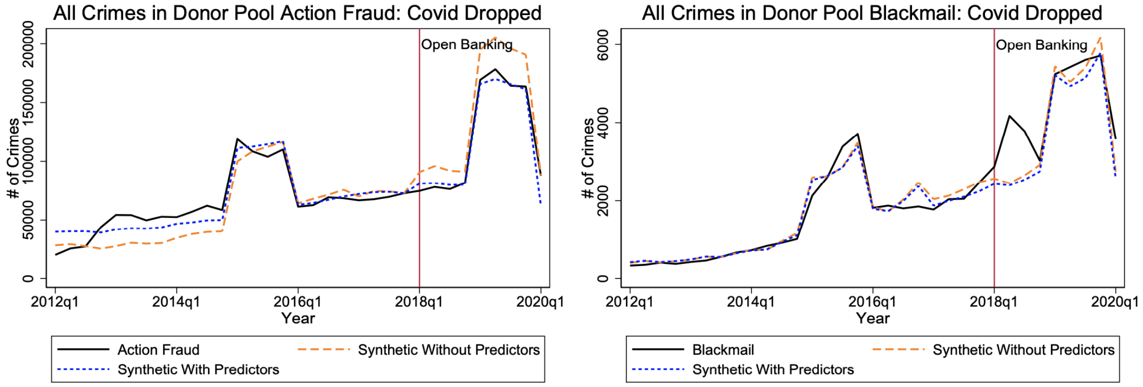


Figure 7. Leaving Out Test for Robustness

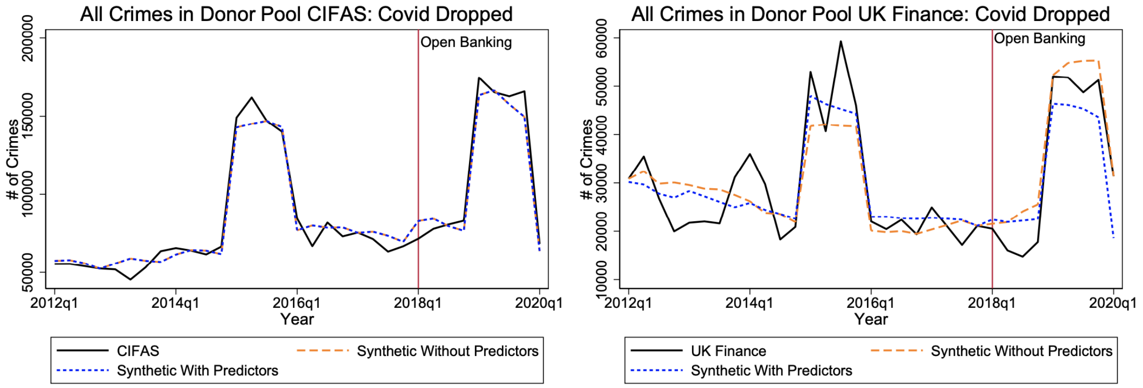
The results of expanding the donor pool to include all types of crimes, not just those that are economic and financial, can be visualized in figures 8 and 9 below. The results of expanding the donor pool are as expected. They show that expanding the donor pool does not change the magnitude of the effect of Open Banking Policies on the treated units. When using predictors, all post-treatment effects are positive. Although, given modest increases of 4.65 percent, 3.71 percent, and 6.03 percent for Action Fraud, CIFAS, and UK Finance respectively, the impact was minimal. These increases are so small that they are effectively zero as they can be explained by population increase. In some cases, such as Action Fraud and UK Finance without predictors, there is a negative effect of Open Banking measured. These results are important as they support the consensus in the literature that expanding the donor pool does not greatly alter the results of the synthetic control model.



(a) All Crimes Action Fraud

(b) All Crimes Blackmail

Figure 8. Expanded Donor Pool - Action Fraud & Blackmail



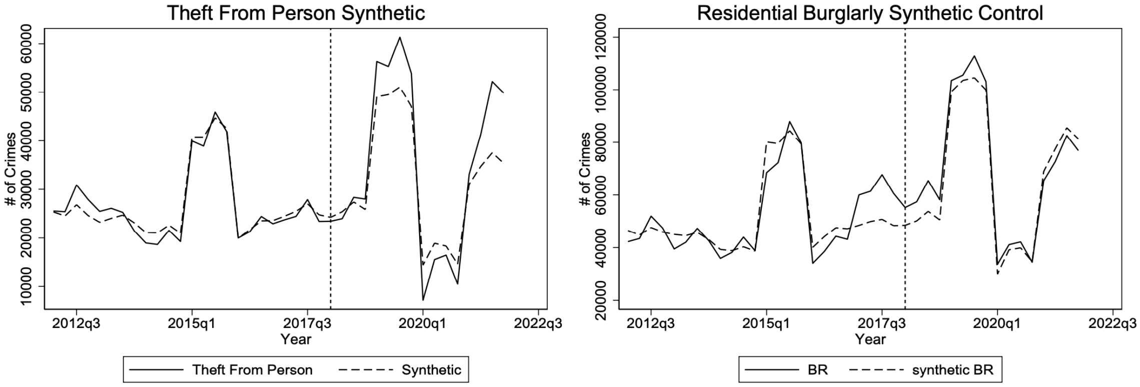
(a) All Crimes CIFAS

(b) All Crimes UK Finance

Figure 9. Expanded Donor Pool - CIFAS & UK Finance

Finally, robustness can be checked using placebo testing. Four types of placebo tests have been conducted in this paper. The first is done by running the synthetic control on an untreated crime that should have been unaffected by Open Banking [Abadie (2021)]. Robustness is confirmed when untreated crimes are unaffected by Open Banking policies. Additionally, the synthetic control method can be run without predictors. If dropping the predictors does not significantly impact the weighting of the synthetic units this also shows robustness. Further, the synthetic control method can be run on an expanded donor pool of crimes. Expanding the donor pool to include non financial and economic crimes, while threatening identification, should not drastically alter the results if they are robust. Lastly, time periods can be dropped to check the robustness of the results. If dropping time periods significantly changes the estimates of the model than the results are not robust.

Placebo testing was conducted by running the synthetic control method on untreated crimes from the donor pool. The crimes of "Theft From the Person and Residential Burglary" were chosen. As seen in figure 10 below, the post-treatment effect on types of crimes is essentially zero. While both crimes exhibit a spike in 2019 due to the aforementioned decrease in civil service funding, the average of the treatment effect compared to the pre-treatment average number of crimes is virtually zero. Thus, running synthetic control on untreated crimes has provided additional robustness to the analysis by showing the untreated crimes in the donor pool are unaffected by Open Banking.



(a) Theft From Person

(b) Residential Burglary

Figure 10. Placebo Test

VII. Conclusion

This paper's analysis finds evidence that Open Banking leads to increased magnitudes of certain types of crimes, particularly blackmail and fraud. All models of synthetic control find a positive impact of Open Banking on fraud and blackmail. In some specifications fraud is less significantly linked to Open Banking but in all cases the relationship is positive. The findings of this study are significant as the magnitude of the impact of Open Banking on economic and financial crime was previously ambiguous. While some results indicate there may be little to no impact of Open Banking, there is no evidence that Open Banking will lead to decreased levels of crime. The results of this paper should be interpreted by policymakers as a sign to proceed with caution. Implementing or expanding Open Banking could potentially exacerbate fraud and lead to consequences that outweigh the benefits. It is recommended that the consequences of Open

Banking be further studied before countries implement or expand their current Open Banking regimes.

REFERENCES

[Abadie 2021] Abadie, Alberto: Using Synthetic Controls: Feasibility, Data Requirements, and Methodological Aspects. In: *Journal of Economic Literature* 59 (2021), 06, S. 391–425

[Anderson and Moore 2006] Anderson, Ross ; Moore, Tyler: The Economics of Information Security. In: *Science* 314 (2006), 11, S. 610

[Brodsky and Oakes 2017] Brodsky, Laura ; Oakes, Liz: Data sharing and open banking. In: *McKinsey Company Articles* 11 (2017), Sept. – URL `https://www.ourperspectives.com/article/345-data-sharing-and-open-banking`

[Buckley et al. 2016] Buckley, Ross ; Arner, Douglas ; Barberis, Janos: The Evolution of Fintech: A New Post-Crisis Paradigm? In: *Georgetown Journal of International Law* 47 (2016), 01, S. 1271–1319

[FTC 2022] FTC: New Data Shows FTC Received 2.8 Million Fraud Reports from Consumers in 2021. In: *Federal Trade Commission Press Release* (2022), Feb. – URL `https://www.ftc.gov/news-events/news/press-releases/`

[Gozman et al. 2018] Gozman, Daniel ; Hedman, Jonas ; Sylvest, Kasper: Open banking: Emergent roles, risks opportunities. In: *26th European Conference on Information Systems, Association for Information Systems - AIS Electronic Library (AISeL)* (2018). – URL `https://aisel.aisnet.org/ecis2018`$_rp$

[Kunreuther and Heal 2003] Kunreuther, Howard ; Heal, Geoffrey: Interdependent Security. In: *Journal of Risk and Uncertainty* 26 (2003), 02, S. 231–49. ISBN 978-1-4419-5428-2

[Monica-Violeta and Sorin 2020] Monica-Violeta, Achim ; Sorin, Borlea: *Economic and Financial Crime: Theoretical and Methodological Approaches.* 08 2020. – 1–71 S. – ISBN 978-3-030-51779-3

[Monica-Violeta et al. 2021] Monica-Violeta, Achim ; Sorin, Borlea ; Vaidean, Viorela: Does technology matter for combating economic and financial crime? A panel data study. In: *Technological and Economic Development of Economy* 27 (2021), 01, S. 1–39

[OpenBanking.org 2022] OpenBanking.org: 5 million users – open banking growth unpacked. In: *Open Banking Limited Press Release* (2022), Feb. – URL `www.openbanking.org.uk/news/5-million-users-open-banking-growth-unpacked/`

[Price-Waterhouse-Cooper 2022] Price-Waterhouse-Cooper: Protecting the perimeter: The rise of external fraud. In: *PwC's Global Economic Crime and Fraud Survey 2022* (2022). – URL `https://www.pwc.com/gx/en.html`

[Shi et al. 2021] Shi, Claudia ; Sridhar, Dhanya ; Misra, Vishal ; Blei, David: On the Assumptions of Synthetic Control Methods. (2021), 12

[Suryono et al. 2020] Suryono, Ryan R. ; Budi, Indra ; Purwandari, Betty: Challenges and Trends of Financial Technology (Fintech): A Systematic Literature Review. In: *Information* 11 (2020), Nr. 12. – URL `https://www.mdpi.com/2078-2489/11/12/590`. – ISSN 2078-2489

[Zhang et al. 2024] Zhang, Leting ; Wattal, Sunil ; Pang, Min-Seok: Does Sharing Make My Data More Insecure? An Empirical Study on Health Information Exchange and Data Breaches. In: *MIS Quarterly* 48 (2024), 09

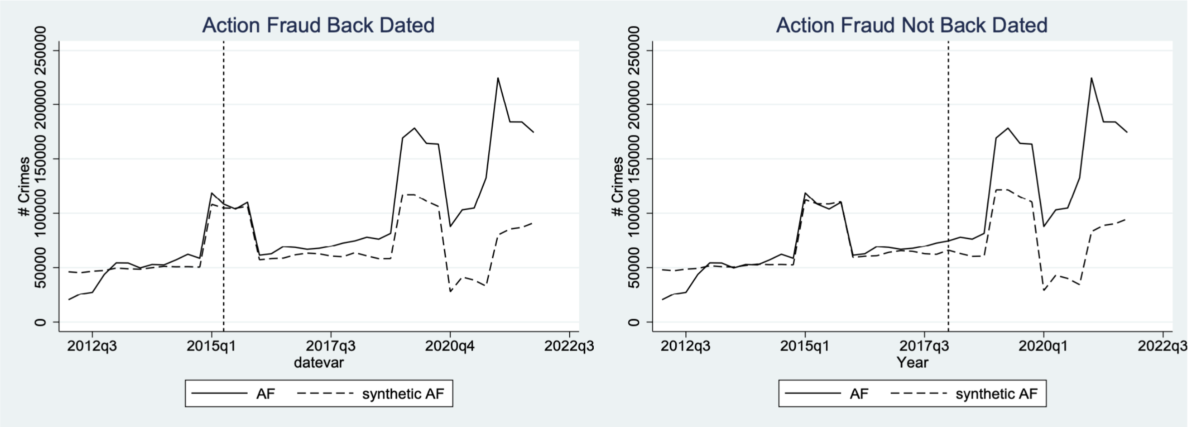
APPENDIX

Table A1—Summary Statistics of Key Variables

Variable	Obs	Mean	Std. Dev.	Min	Max
Number of Crimes	1440	22963	37887	21	224584
Unemployment	1440	5.34	1.4	3.8	8.2
GDP Per Capita	1440	42455	2001	34508	45016
Population	1440	65735	1202	63600	67473
Crime Per Capita	1440	0.35	0.0003	0.0003	3.34
Crime/GDP Per Capita Ratio	1440	0.54	0.88	0.0005	5.59
Crime/Unemployment Ratio	1440	4261	8445	2.6	52371

Table A2—List of All Economic and Financial Crimes Recorded

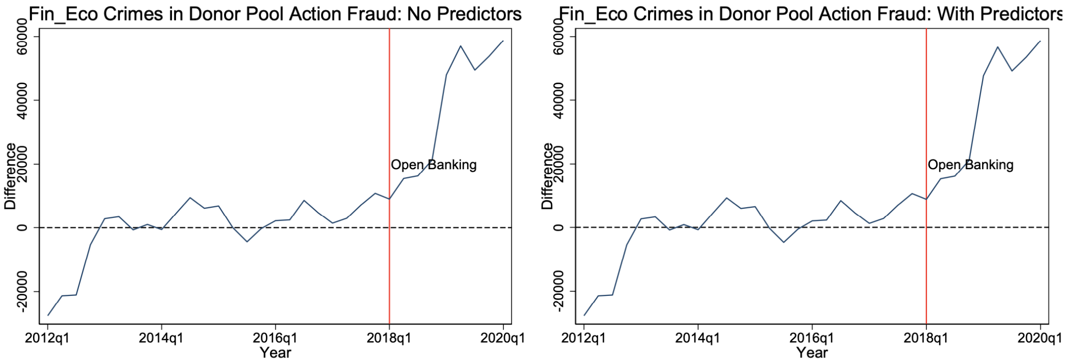
Economic and Financial Crime Recorded in Data Set
Aggravated burglary business and community, residential or non-dwelling building
Aggravated vehicle taking
Attempted burglary business and community or residential
Blackmail
Burglary business and community or residential
Dishonest use of electricity
Distraction or attempted distraction burglary residential
Exploitation of prostitution
Fraud offences recorded by Action Fraud, CIFAS or UK Finance
Going equipped for stealing, etc.
Handling stolen goods
Making off without payment
Making, supplying or possessing articles for use in fraud
Other drug offences, forgery, theft
Profiting from or concealing knowledge of the proceeds of crime
Robbery of business property
Shoplifting
Soliciting for the purposes of prostitution
Theft by an employee, from automatic machine or meter, from the person or from vehicle
Theft of mail
Theft or unauthorized taking of a pedal cycle or motor vehicle
Trafficking in controlled drugs



(a) Action Fraud Back Dated

(b) Differences Predictors

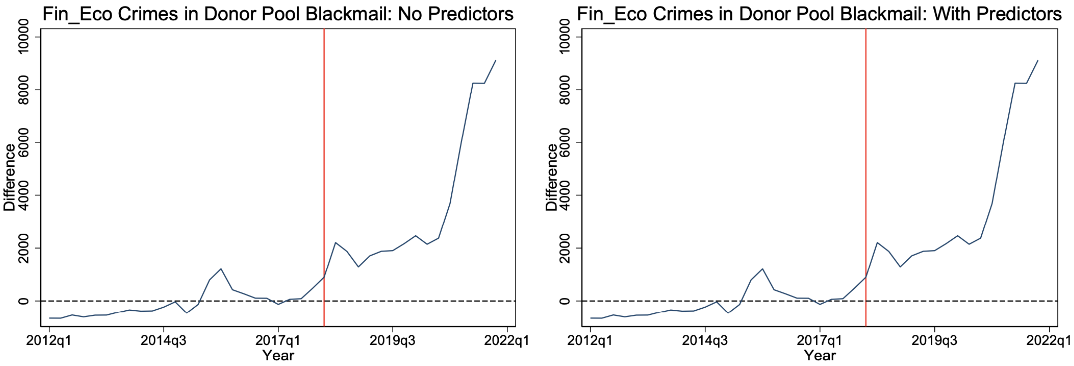
Figure A1. Back Dating Robustness Visualization



(a) Differences No Predictors

(b) Differences Predictors

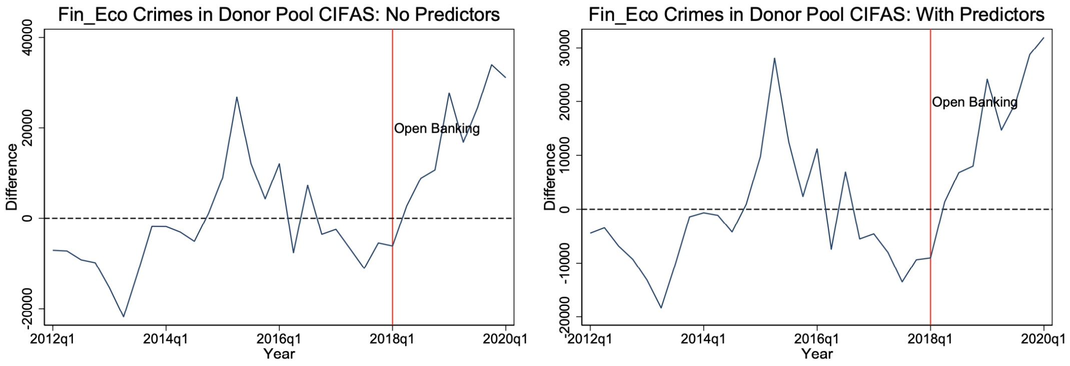
Figure A2. Action Fraud Main Specification Differences



(a) Differences No Predictors

(b) Differences Predictors

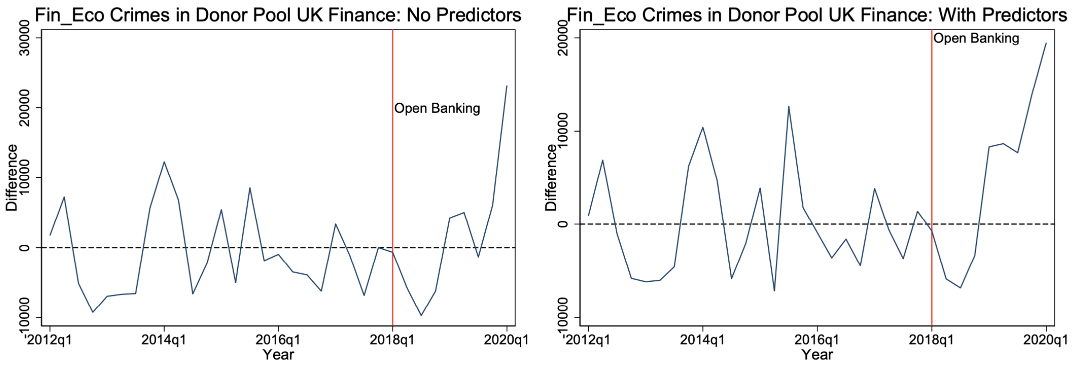
Figure A3. Blackmail Main Specification Differences



(a) Differences No Predictors

(b) Differences Predictors

Figure A4. CIFAS Main Specification Differences



(a) Differences No Predictors

(b) Differences Predictors

Figure A5. UK Finance Main Specification Differences