NORTH CAROLINA BANKING INSTITUTE

Volume 26 | Issue 1 Article 17

3-1-2022

Open Banking: The CFPB Should Follow the European Regulatory Regime

Sara C. Markov

Open Banking: The CFPB Should Follow the European Union Regulatory Regime

I. INTRODUCTION

Fifty-two percent of Americans say they have "no clue" what Open Banking is.[1] Despite this, Open Banking is *absolutely* happening in the U.S., just not in the same manner as in the European Union ("EU").[2] The term "Open Banking" refers to the general concept of consumers sharing their financial data with third parties through the use of software that enables two applications to communicate with each other.[3] Use of this software—known in the marketplace as an Application Program Interface ("API")[4]—is becoming increasingly common within the financial services sector.[5] A well-known example of API technology is Venmo, an app which enables consumers to link their bank accounts to the app in order to send and receive money to and from friends.[6]

---

1. Linda Yang, *GoCardless Launches Open Banking Payments, Offering Businesses a New Alternative to Taking One-Off Payments*, GOCARDLESS (Apr. 26, 2021), https://gocardless.com/en-us/blog/open-banking-payments-release/ [https://perma.cc/ZV66-6FH9] (According to independent research from GoCardless, "half of Americans (52%) say they have 'no clue' what Open Banking is.").

2. *See* Miriam Cross, *What Will it Take for Open Banking to Take Hold in the U.S.?,* AM. BANKER (June 30, 2021, 9:30 PM), https://www.americanbanker.com/podcast/what-will-it-take-for-open-banking-to-take-hold-in-the-u-s [https://perma.cc/4CJB-X5X7] (describing how Open Banking in the U.S. is market-driven, as opposed to how Open Banking in the EU is driven by regulation).

3. John Egan, *What is Open Banking?,* U.S. NEWS (June 2, 2021, 4:17 PM), https://money.usnews.com/banking/articles/what-is-open-banking [https://perma.cc/L6VZ-YFZT].

4. *Id.* ("An API is a software that enables two applications to communicate with each other.").

5. *See* Cross, *supra* note 2 (explaining that Experian is already using Open Banking technology to provide consumers with an alternative way to demonstrate creditworthiness and provide a holistic view of their finances); *see also* CARPENTER WELLINGTON PLLC, *Fintech Acquisitions Focus of Payment Companies Visa and Mastercard*, LEXOLOGY (Aug. 21, 2020), https://www.lexology.com/library/detail.aspx?g=200132f9-e6ea-4c4d-b75e-3e7d8fb872f1 [https://perma.cc/T27F-S2UY] (noting that Mastercard and Visa have recently acquired Fintech companies to offer technology that allows consumers to share their financial data with third parties).

6. *See* Ben Gran & Mitch Strohm, *Venmo vs. PayPal: Which to Use and When*, FORBES (July 26, 2021, 7:00 AM), https://www.forbes.com/advisor/banking/venmo-vs-paypal/ [perma.cc/5H79-83TG] (explaining that Venmo is one of the most popular apps on the market which allows consumers to connect bank accounts to send and receive money).

In contrast, Open Banking, in the regulatory sense,[7] emerged from the EU's regulation of its financial services sector.[8] Since 2008, regulators in the EU have tried to combat risk within the financial industry by imposing higher reporting obligations[9] and requiring all financial service providers to offer standardized APIs that allow consumers to securely share their financial data with third parties.[10] The EU has also imposed stringent regulations surrounding data sharing practices, requiring institutions to collect, share, and protect data in a certain manner.[11] While the Open Banking technology in both the U.S. and the EU is relatively similar, the development of this technology in the U.S. is being driven by the market, not regulation.[12]

This market push towards Open Banking is largely driven by consumers' desire for services that make managing their financial lives

7. It is important to note that regulation was not the only driving force behind the adoption of Open Banking in the EU; consumer demand, competition in the market, and technological advances also had a hand in the emergence of Open Banking in the EU. *See* Nikola Jelicic et al., *Open Banking—Far More than PSD2*, BANKING HUB, https://www.bankinghub.eu/themen/open-banking-far-more-than-psd2 [https://perma.cc/2PS2-458S] (noting that regulation was "not the only trend forcing a shift of the sector towards Open Banking").

8. *See* Douglas W. Arner et al., *The Future of Data-Driven Finance and Regtech: Lessons from EU Big Bang II*, 25 STAN. J. OF L. BUS. & FIN. 245, 254 (2020) ("EU financial regulatory reporting requirements have driven digitization and datafication of finance and its regulation, causing a massive increase in RegTech and the transition to data-driven finance in Europe's traditional financial services industry.").

9. The EU requires financial intermediaries to report data on their decisions, activities and exposures to European regulators. *See id.* (discussing the "RegTech Revolution" in the EU financial industry and explaining how heightened reporting requirements has forced financial institutions to implement new technology to remain in compliance).

10. Council Directive, 2015/2366, art. 82(1)(c), 2015 O.J. (L 337) 58 (E.U.), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015L2366 [https://perma.cc/3GA3-K7LC].

11. EU General Data Protection Regulation (GDPR): Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data and Repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) 1, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679 [https://perma.cc/DWP9-4Z2K].

12. *See* Cross, *supra* note 2 ("But even though the U.S. doesn't have those rules doesn't mean it doesn't functionally have Open Banking already – it's just driven by the market.").

easier.[13] To meet this demand, financial service providers and fintechs[14] are implementing API technology, enabling consumers to seamlessly share their financial data across platforms, applications, and industries.[15] This technology eliminates the need for consumers to manually input financial information when opening a new account or applying for a mortgage, and in turn, creates an alternative way to demonstrate creditworthiness to creditors and provides consumers with a holistic view of their finances.[16]

Despite many potential benefits of sharing financial data,[17] there is an inherent risk of consumer data being misappropriated or ending up in the hands of cybercriminals.[18] In light of several recent high-profile cyber-attacks in the U.S.,[19] protecting sensitive data should be one of the

---

13. *See* FIN. TECH. PARTNERS, OPEN BANKING: REARCHITECTING THE FIN. LANDSCAPE 1, 134 (March 2021), https://ftpartners.docsend.com/view/wdfyv732df2qyhb6 [https://perma.cc/MRH4-7TM8]

("Your research also found that consumers are generally receptive to Open Banking, with the highest amount of interest coming from millennials and Gen Z.").

14. For the purposes of this Note, "fintech" refers to the very general idea of "financial technology" without diving into the granular industries encompassed within the term. *See* Stephanie Walden, *What is Fintech and How Does it Affect How I Bank?*, FORBES (Aug. 3, 2020, 7:00 PM), https://www.forbes.com/advisor/banking/what-is-fintech/ [https://perma.cc/T6ZT-AAWM] (defining fintech as a "catch-all term for any technology that's used to augment, streamline, digitize or disrupt traditional financial services").

15. *See* CARPENTER WELLINGTON PLLC, *supra* note 5 (explaining that Mastercard and Visa's fintech acquisitions "are a sign that traditional financial institutions are embracing the need for technology-focused payment solutions").

16. *See* Egan, *supra* note 3 (providing an overview of potential benefits of Open Banking).

17. Some potential benefits of Open Banking technology are: (1) the ability to easily send mortgage lenders sensitive financial information by granting access to consumer banking information; (2) the ability to quickly open a new financial account without manually entering consumer information; (3) more personalized financial products; (4) inclusive credit; (5) the provision of a holistic view of consumer finances. *See id.* (discussing some of the potential benefits of Open Banking technology).

18. *See id.* ("James E. Lee, chief operating officer of the Identity Theft Resource Center, says the rise of APIs trouble him because of the technology's security vulnerabilities, and the relative lack of scrutiny that APIs receive.").

19. *See Hackers Steal $600m in Major Cryptocurrency Heist*, BBC (Aug. 11, 2021), https://www.bbc.com/news/business-58163917 [https://perma.cc/C7YH-JBYS] (reporting on the recent Bitcoin heist); *see also* Penny Crosman, *'It's Very Scary': Small Banks Quietly Hit by Ransomware Attacks*, AM. BANKER (May 24, 2021), https://www.americanbanker.com/news/its-very-scary-small-banks-quietly-hit-by-ransomware-attacks [https://perma.cc/Z6FU-N762] (reporting on recent attacks on three small, unnamed banks); *see also* Marc Rotenberg, *To Prevent Data Breaches Like Capital One, Congress Needs to Act*, CNN (July 30, 2019), https://www.cnn.com/2019/07/30/perspectives/capital-one-hack-prevent/index.html [https://perma.cc/K3Z4-HM5L] (reporting on the recent Capital One data breach and how Congress needs to act to prevent future attacks).

top concerns for the financial services industry.[20] Currently, the patchwork of regulation, consumer protection laws, and outdated authentication methods leave much to be desired in protecting this sensitive data.[21]

This Note considers the role of Open Banking in the U.S. and how the implementation of uniform regulations may make data sharing safer and eliminate the uncertainty surrounding compliance and accountability within the market.[22] In the current marketplace, there are major questions surrounding who is responsible in the event of a data breach, especially when multiple marketplace participants are involved in a single transaction.[23] Eliminating some of these uncertainties for developers will, in turn, promote innovation and competition within the financial services industry,[24] making credit and financial products more affordable for consumers.[25] Regulatory reform will also provide the U.S. with an opportunity to raise the baseline standard for data protection and move away from the current patchwork of regulation.

This Note proceeds in six parts. Part II introduces the concept of Open Banking and examines the benefits and risks generally associated with Open Banking technology.[26] Part III provides an in-depth

20. *See* Alastair Johnson, *Open Banking, Open Risk: How to Eliminate Fraud in the Future of Finance*, FORBES (Nov. 26, 2020, 11:37 AM), https://www.forbes.com/sites/alastairjohnson/2020/11/26/open-banking-open-risk-how-to-eliminate-fraud-in-the-future-of-finance/?sh=1a5d7bef6eff [https://perma.cc/J478-HZM3] (explaining the risk of data security remains "potentially significant" within the Open Banking market).

21. *See* Saavedra-Lim, *Look Out for Risks in Open Banking!*, TERADATA (June 21, 2021), https://www.teradata.com/Blogs/Look-Out-for-Risks-in-Open-Banking [https://perma.cc/J478-HZM3] (providing an overview of the risks associated with Open Banking technology); *see also* Johnson, *supra* note 20 ("The biggest danger for the banks is they have provided the service as agreed with the regulator, but once beyond their walls, privacy and security can go awry.").

22. *See* Jacob Kosoff, *Europe's New API Rules Lay Groundwork for Regulating Open Banking*, BLOOMBERG (Jan. 27, 2020), https://www.bloomberg.com/professional/blog/europes-new-api-rules-lay-groundwork-for-regulating-open-banking/ [https://perma.cc/Y78G-5F5R] ("Implementing existing laws within an Open Banking business model will require legal interpretation and regulatory innovation.").

23. *See* Saavedra-Lim, *supra* note 21 (providing an overview of the risks associated with Open Banking technology); *see also* Johnson, *supra* note 20 ("The biggest danger for the banks is they have provided the service as agreed with the regulator, but once beyond their walls, privacy and security can go awry.").

24. Kosoff, *supra* note 22.

25. *See* Exec. Order No. 14036, 86 Fed. Reg. 36,987 (July 9, 2021) ("In the financial-services sector, consumers pay steep and often hidden fees because of industry consolidation.").

27. *See infra* Part II.

comparison of Open Banking in the U.S. versus the uniformly regulated Open Banking market in the EU.[27] Part IV considers the role of Open Banking technology in cybersecurity and data autonomy.[28] Part V explores how a regulated market might give a consumer more control of their data, provide a safer way to share data, and promote competition within the marketplace.[29] Finally, Part VI provides a brief conclusion.[30]

II. BACKGROUND

A. An Introduction to Open Banking

The definition of Open Banking largely depends on geographic location and the context in which the term is used.[31] In the EU, Open Banking generally refers to the regulated marketplace of data sharing across platforms, as opposed to the practice of data sharing itself.[32] In the U.S., however, Open Banking generally refers to the practice of consumers sharing their financial information in real-time with third-party vendors through the use of APIs.[33]

Despite the lack of regulation, this practice of data sharing across platforms using API technology is nothing new.[34] For example, Experian Boost implemented the use of API technology in early 2019, allowing consumers to use unconventional types of payment histories[35] to increase their credit scores.[36] This alternative way to demonstrate

27. *See infra* Part III.
28. *See infra* Part IV.
29. *See infra* Part V.
30. *See infra* Part VI.
31. *See* Cross, *supra* note 2 (exploring the difference between the market driven Open Banking and regulation driven Open Banking).
32. *Id.*
33. *See* Egan, *supra* note 3 ("Through the open-banking concept, you allow third-party financial services companies – with your permission – to access your personal financial data. This is accomplished with technology known as application programming interfaces, or APIs. An API is software that enables two apps to communicate with each other.").
34. *See* Cross, *supra* note 2 (providing examples of Open Banking technology in the U.S., including Experian Credit Boost).
35. Stefan Lembo Stolba, *Does Experian Boost Work?*, EXPERIAN (July 20, 2020), https://www.experian.com/blogs/ask-experian/does-experian-boost-work/ [https://perma.cc/JU9W-V66S] (explaining that Netflix monthly payments, payroll histories, and rent payments are among those unconventional forms of financial histories used by Experian Boost).
36. *Id.*

creditworthiness can make credit more accessible to consumers who might not have the credit history that traditional lenders desire.[37]

Inclusive credit is just one of the many potential benefits of Open Banking technology.[38] When implemented properly, this technology can give the consumer more control over how their data is used and shared.[39] When consumers can share their financial data with other banks and third-party servicers, it eliminates the need to manually input financial information when opening a new account or applying for a mortgage, making the process faster and more convenient.[40] Open Banking technology also gives consumers a holistic overview of their finances, making it easier to manage their finances without having to use multiple applications.[41] For example, Mint is an app which utilizes API technology and enables consumers to connect all of their financial accounts so they can see their "complete financial picture" on one screen.[42] This comprehensive view of finances not only helps consumers with financial planning but also enables businesses to offer personalized financial products to their customers.[43]

It is prudent, however, for consumers to approach Open Banking technology and its promised benefits with some level of skepticism.[44] The more engrained Open Banking technology and data sharing becomes in our day-to-day lives, the greater the risk for consumer data being compromised.[45] Consumers should be wary about who they share their data with and what security measures companies have in place to ensure their data is protected.[46] While data security is one of the top concerns

37. *See* Egan, *supra* note 3 (explaining how Open Banking technology gives people with "little to no credit history" better access to credit).

38. *See id.* (providing an overview of the many potential benefits of Open Banking technology).

39. *Id.*

40. *Id.*

41. *Id.*

42. *See What is Mint, and How Does it Work?,* MINT, https://mint.intuit.com/how-mint-works/ [https://perma.cc/GE7J-RWZF] ("Easily connect all your accounts. From cash and credit to loans and investments, you can see your complete financial picture in Mint.").

43. Egan, *supra* note 3.

44. *See id.* ("While Open Banking delivers a number of potential benefits and financial services providers insist it isn't safe, this concept also may trigger some concerns.").

45. *See* Walden, *supra* note 14 (exploring the risks associated with fintech and how engaging with fintechs may lead to unwanted exposure).

46. *See* Egan, *supra* note 3 (providing an overview of the potential risks associated with Open Banking technology); *see also* Walden, *supra* note 14 ("The idea that fintechs adhere to some kind of higher moral standard than the big banks is also proving largely illusory."); *see also API Attacks Become More Common as Software Grows in Popularity*, IDENTITY

associated with the practice of data sharing, it is not the only risk consumers should consider.[47]

Concerns surrounding data ownership are also particularly relevant to the practice of data sharing.[48] When consumer data is transferred across multiple platforms, industries, and institutions, there are questions of who owns that data, who is required to protect that data, and what can be done with that data.[49] For example, can a consumer's data be sold or used for marketing purposes without the consumer's consent?[50] These questions remain largely unanswered by current regulation in the U.S., creating massive risk for financial institutions and technology firms that are trying to enter the Open Banking market.[51]

Despite these risks, an estimated 80–100 million consumers in North America have shared their data with a third-party application or service through the use of Open Banking technology.[52] The U.S. federal government has done very little to meet this market demand for Open Banking with any uniform regulation.[53] Conversely, the EU has heavily and uniformly regulated its Open Banking market for several years with the goal of making the marketplace more competitive and safer for both consumers and providers.[54]

THEFT RES. CTR. (June 4, 2021) https://www.idtheftcenter.org/api-attacks-become-more-common-as-software-grows-in-popularity/ [https://perma.cc/4BR9-VJ7T] (explaining that Facebook, LinkedIn, Peloton and Microsoft all experienced data breaches that were the result of flawed API technology).

47. *See* Egan, *supra* note 3 (discussing the other concerns surrounding Open Banking).

48. *See* Saavedra-Lim, *supra* note 21 (providing an overview of the risks associated with Open Banking technology); *see also* Johnson, *supra* note 20 ("The biggest danger for the banks is they have provided the service as agreed with the regulator, but once beyond their walls, privacy and security can go awry.").

49. *Id.*

50. While consumers may enjoy the convenience of Open Banking technology, there is a risk that financial institutions collecting consumer data inundate consumers with a barrage of marketing. *See* Saavedra-Lim, *supra* note 21 (providing an overview of the risks associated with Open Banking technology); *see also* Egan, *supra* note 3.

51. Egan, *supra* note 3.

52. *See* Cross, *supra* note 2 ("We estimate that in North America somewhere between 80 and 100 million consumers had shared data with a third-party app or service either on a one-time basis or an on-going basis.").

53. *See id.* ("In the U.S., there is no regulations defining Open Banking or its interpretation of what Open Banking is.").

54. While the EU enacted Open Banking regulation in early 2019, it was not fully enforced in its current capacity until 2020. *See* Gaynor, *Payment Services Directive 2- An Overview*, J.P. MORGAN, https://www.jpmorgan.com/europe/merchant-services/insights/PSD2-all-you-need-to-know [https://perma.cc/C6DM-RHNY] ("In October 2019, the European Banking Authority (EBA) released an opinion stating the revised deadline for migration to SCA has been set at 31 December 2020.").

III. A COMPARISON OF OPEN BANKING IN THE U.S. AND EU

A. Open Banking in the EU

The European Union originally entered the Open Banking regulatory arena in 2009 by implementing Payment Service Providers Directive 1 ("PSD1"),[55] which requires banks to create APIs and open those APIs to third-party developers.[56] The law has since evolved into Payment Services Providers Directive 2 ("PSD2"), which was adopted in 2018.[57] The main goals of PSD2 were to address "significant challenges from a regulatory perspective" surrounding areas of the payment markets and to address the regulatory gaps of PSD1.[58] This directive contained two key elements: (1) Strong Customer Authentication ("SCA"), and (2) two types of new regulated service providers.[59]

The primary goal of the SCA requirement is to reduce payment fraud without creating an inconvenience for the consumer using the technology.[60] This is a form of two-factor authentication, requiring consumers to provide two pieces of information to prove their identity.[61] For example, a consumer could use their fingerprint and the last four digits of their social security number[62] to properly authenticate their identity and satisfy the SCA requirements.[63]

---

55. Council Directive 2007/64, 2007 O.J. (L 319) 1 (EC) https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2007:319:0001:0036:en:PDF [https://perma.cc/KJ7M-VLT8].

56. Kosoff, *supra* note 22.

57. Council Directive, 2015/2366, art. 82(1)(c), 2015 O.J. (L 337) 58 (E.U.) https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015L2366 [https://perma.cc/3GA3-K7LC].

58. *Id.*

59. *Id.*

60. Gaynor, *supra* note 54.

61. *See* Council Directive, 2015/2366, art. 82(1)(c), 2015 O.J. (L 337) 58 (E.U.), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015L2366 [https://perma.cc/3GA3-K7LC] ("Strong customer authentication means an authentication based on the use of two or more elements categorized as knowledge (something only the user knows), possession (something only the user possesses) and inherence (something the user is) that are independent, in that the breach of one does not compromise the reliability of the others, and is designed in such a way as to protect the confidentiality of the authentication data.").

62. European countries also utilize identification numbers, although not referred to as social security numbers. For example, the UK utilizes a "National Insurance Number." *Apply for a National Insurance Number*, GOV.UK, https://www.gov.uk/apply-national-insurance-number [https://perma.cc/5FYW-R9QC].

63. *See* Gaynor, *supra* note 54 (explaining that some transactions are exempt from this authentication requirement, such as low value transactions).

Under the second element of PSD2, two new regulated service providers emerged: Payment Initiation Service Providers ("PISPs"), and Account Information Service Providers ("AISPs").[64] PISPs are able to initiate payments directly from a consumer's account once a customer has consented.[65] AISPs allows users to see all of their financial information in one place.[66] This development of new third-party payment providers gives customers more banking and payment options and allows merchants to utilize customer information to make risk assessments.[67]

The enactment of PSD2 streamlined fintech companies' access to bank data, eliminating the legal uncertainty surrounding new partnerships between banks and fintechs.[68] The legal certainty in the EU may encourage investment and innovation in EU countries rather than the U.S., resulting in the U.S. losing its historically competitive edge in the market.[69] By creating uniform standards and reducing uncertainty, Open Banking regulation also allows smaller tech companies, which might not have the same resources as their larger competitors, to compete for greater market share.[70]

Alongside PSD2, the EU enacted the General Data Protection Regulation ("GDPR").[71] The GDPR was designed to increase data security protocols and prevent data breaches through stricter regulations.[72] The GDPR addresses many of the data security and

64. *See* Council Directive, 2015/2366, art. 82(1)(c), 2015 O.J. (L 337) 58 (E.U.), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015L2366 [https://perma.cc/3GA3-K7LC] ("Strong customer authentication means an authentication based on the use of two or more elements categorized as knowledge (something only the user knows), possession (something only the user possesses) and inherence (something the user is) that are independent, in that the breach of one does not compromise the reliability of the others, and is designed in such a way as to protect the confidentiality of the authentication data.").

65. Gaynor, *supra* note 54.

66. *Id.*

67. *Id.*

68. *See* Kosoff, *supra* note 22 (explaining that PSD2 is more friendly to fintech companies as it "streamlines access to a growing network of bank data," as opposed to fintechs in the U.S. having to create individual data sharing agreements with each bank partner).

69. *See id.* (warning that the U.S. should take notice of PSD2 because standardization of Open Banking could give the European banking system a competitive edge).

70. *See id.* (explaining that without standardization of Open Banking, fintechs must create "individual data sharing agreements" which can be resource intensive).

71. *See* Ben Wolford, *What is the GDPR, the EU's New Data Protection Law?*, GDRP, https://gdpr.eu/what-is-gdpr/ [https://perma.cc/LGX8-YRW4] (stating the GDRP was enacted in May of 2018).

72. EU General Data Protection Regulation (GDPR): *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural*

protection issues surrounding Open Banking that are not directly addressed by PSD2.[73] The GDPR focuses on: (1) privacy policies being written in "clear straightforward language"; (2) receiving "affirmative consent" from consumers before using their data; (3) more transparency in a data-sharing transaction; (4) consumers having more control and personal rights over their data; and (5) data protection authorities having stronger enforcement powers.[74] Although this regulation was passed by the EU, it applies to any organization, anywhere in the world, that collects data from EU citizens, including U.S. companies.[75]

The far-reaching effects of the GDPR have imposed significant burdens on U.S. companies who are required to comply with its regulations.[76] Over 40% of U.S. companies each spent more than $10 million updating their systems in order to comply with the GDPR.[77] Any noncompliance allows authorities from all over the EU to impose harsh fines against offenders[78]—potentially as much as 4% of the offending company's annual global revenue.[79]

The EU has been firm in its enforcement of GDPR, issuing fines totaling hundreds of millions of euros since its enactment.[80] One of the first companies that the EU fined for violating the regulation was Google;[81] a French regulator issued a 50 million euro fine, ruling that the

---

Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data and Repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) 1, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679 [https://perma.cc/DWP9-4Z2K].

73. *See* Wolford, *supra* note 71 (defining the key regulatory points of the GDRP: data protection, accountability, data security, when you're allowed to process data, consent, and privacy rights).

74. *See* EUR. COMM., *A New Era for Data Protection in the EU: What Changes After May 2018*, 1-3, https://ec.europa.eu/info/sites/default/files/data-protection-factsheet-changes_en.pdf [https://perma.cc/8JPR-76F5] (providing high-level overview of the main objectives of the GDPR).

75. Wolford, *supra* note 71.

76. *See* Crosman, *supra* note 19 ("Of the U.S. companies that completed their compliance work, 40% spent more than $10 million, according to a PwC survey conducted last year.").

77. *Id.*; *see also* Joe DeMarzio, *A Privacy Rest – From Compliance to Trust-Building*, PWC, https://www.pwc.com/us/en/services/consulting/cybersecurity-risk-regulatory/library/privacy-reset.html [https://perma.cc/D54X-BXG2] ("Eighty-eight percent of global companies say that GDPR compliance alone costs their organization more than $1 million annually, while 40% spend more than $10 million.").

78. Wolford, *supra* note 71.

79. Crosman, *supra* note 19.

80. *Three Years of GDPR: The Biggest Fines So Far*, BBC (May 24, 2021), https://www.bbc.com/news/technology-57011639 [https://perma.cc/JMB4-PQSG].

81. *Id.*

company's data processing statements were not easily accessible to consumers.[82] Marriot International Hotels and British Airways were also fined by UK authorities for violating GDPR requirements.[83] Each country has different processes in place for the imposition and collection of these fines, but the GDPR provides a uniform regulatory system that provides standards for whether a violation has occurred in the first place.[84]

After the enactment of PSD2 and GDPR, critics have argued that the objectives of these two laws are in conflict with one another, adding to the compliance burden on financial institutions.[85] PSD2 requires financial institutions to open up their data infrastructures to allow access to consumer data, while the GDPR requires those same institutions to keep personal data safe and protected from unauthorized sharing with other parties.[86] This has led to concerns that compliance with PSD2 may, in some instances, require breaching the GDPR and vice-versa.[87]

For example, under the PSD2, Account Servicing Payment Service Providers ("ASPSP"), namely banks and financial institutions, are required to give access to consumer data as soon as a Third-party Payment Provider ("TPP") makes the request.[88] However, the ASPSP is not entitled to receive any confirmation that the TPP has obtained explicit consent from the consumer to share their data.[89] The GDPR requires that all institutions who share consumer data are required to obtain explicit

82. *Id.*

83. *Id.*

84. *See id*. (explaining that each country's regulators handled the imposition of fines for each company).

85. *See EU: The Interplay of PSD2 and GDPR – Some Select Issues*, TWO BIRDS (Feb. 2019) https://www.twobirds.com/~/media/pdfs/eu-the-interplay-of-psd2-and-gdpr--some-select-issues.pdf [https://perma.cc/ALL9-SSTP] (addressing the conflicting provisions of the GDPR and the PSD2); *see also* Kristof Van Quathem & Sophie Bertin, *GDPR and PSD2: A Compliance Burden for Financial Institutions*, THOMSON REUTERS (Apr. 18, 2018), https://www.cov.com/-/media/files/corporate/publications/2018/04/gdpr_and_psd2_a_compliance_burden_for_financial_institutions.pdf [https://perma.cc/44HU-4XFN] (exploring the additional compliance burden on financial institutions due to the interaction between the PSD2 and the GDPR).

86. *See EU: The Interplay of PSD2 and GDPR – Some Select Issues*, TWO BIRDS (Feb. 2019) https://www.twobirds.com/~/media/pdfs/eu-the-interplay-of-psd2-and-gdpr--some-select-issues.pdf [https://perma.cc/ALL9-SSTP] (addressing the conflicting provisions of the GDPR and the PSD2).

87. *See id*. ("So it is no surprise that as part of PSD2 projects that Bird & Bird have been handling for clients, questions have arisen such as: 'If we comply with the PSD2, surely we will breach the GDPR!?,' and vice versa as part of GDPR projects for payments companies.").

88. *Id.*

89. *Id.*

consent.[90] Therefore, ASPSPs are at risk of breaching the GDPR if explicit consent has not been obtained by the TPP, but if they do not comply with the request for consumer data, they are at risk of breaching the PSD2.[91]

Despite these conflicts, there is a significant overlap in the two pieces of legislation.[92] Both the PSD2 and the GDPR give consumers control and ownership over their data to help them safely and securely manage their digital lives.[93] Companies will have to find the balance between providing consumer data pursuant to the PSD2, with protecting the data in compliance with the GDPR[94]—a potentially costly endeavor.[95] This tension between the PSD2 and GDPR is an issue that should be recognized by any future regulation surrounding data sharing and open banking in the U.S. to prevent any discord between the two.

B. The Lack of Regulation in the U.S.

Unlike the EU, the U.S. has yet to implement any type of uniform Open Banking regulations.[96] Absent regulation, Open Banking continues to evolve under the oversight of financial service providers and existing law.[97] While U.S. regulators have issued Open Banking guidelines,[98] there is currently no uniform policy around sharing or ownership of customer information.[99] Instead, financial institutions must look to the

---

90. *Id.*

91. For a more in-depth examination of the tension between the GDPR and the PSD2, *see id*. (exploring the conflicting provisions of each piece of legislation).

92. *PSD2 v GDPR: Can Finance Firms Reconcile the Incompatible?*, AON https://www.aon.com/unitedkingdom/insights/psd2-vs-gdpr.jsp [https://perma.cc/JQ4E-7BT9].

93. *Id.*

94. *Id.*

95. *See* Crosman, *supra* note 19 (discussing the financial effects of the GDPR on U.S. companies).

96. *See* Kosoff, *supra* note 22 (explaining that there are currently no requirements in the U.S. that mandates banks to adopt certain open-banking standards).

97. *See* Egan, *supra* note 3 ("In the U.S., financial services providers largely oversee Open Banking on their own.").

98. CONSUMER FIN. PROT. BUREAU, *Consumer-Authorized Financial Data Sharing and Aggregation: Stakeholder Insights That Inform the Consumer Protection Principles* (Oct. 18, 2017), https://files.consumerfinance.gov/f/documents/cfpb_consumer-protection-principles_data-aggregation_stakeholder-insights.pdf [https://perma.cc/R3RA-XEEQ].

99. *See* Cesare Fracassi & William Magnuson, Data Autonomy, 74 VAND. L. REV. 327, 347 (2021) (explaining that while data ownership, on its face, might seem straightforward,

"fragmented" financial regulatory system and consumer protection laws to ensure data sharing practices and Open Banking technology are compliant with the existing legal framework.[100]

At the federal level, financial regulators are grouped into four main areas: (1) depository regulators,[101] (2) securities markets regulators,[102] (3) government-sponsored enterprise regulators,[103] and (4) consumer protection regulators.[104] To address any gaps that may be present between regulatory groups, Congress created the Financial Stability Oversight Council ("FSOC") in 2010.[105] Even with the many regulators overseeing the financial services sector, none have addressed Open Banking via express regulation.[106] However, the Consumer Financial Protection Bureau ("CFPB" or the "Bureau") and Executive Branch have, however, made regulatory efforts surrounding Open Banking with the goal of making data sharing safer and more accessible as well as promoting competition within the financial services industry.[107] These efforts are discussed more fully below.

---

there is a lot of ambiguity surrounding who owns consumer data in the financial industry, largely in part due to legal and policy issues).

100. *See* CONG. RSCH. SERV., R44918, *Who Regulates Whom? An Overview of the U.S. Financial Regulatory Framework* (2020), https://sgp.fas.org/crs/misc/R44918.pdf [https://perma.cc/T692-PFX6] ("The financial regulatory system has been described as fragmented, with multiple overlapping regulators and a dual state-federal regulatory system.").

101. Depository regulators include the Office of the Comptroller of Currency ("OCC"), Federal Deposit Insurance Corporation ("FDIC"), Federal Reserve for Banks, and National Credit Union Administration ("NCUA"). *Id.*

102. Securities markets regulators include – Securities and Exchange Commissions (SEC) and Commodity Futures Trading Commission (CFTC). *Id.*

103. Government- sponsored enterprise regulators include – Federal Housing Finance Agency (FHFA) and Farm Credit Administration (FCA). *Id.*

104. Consumer protection regulators include the Consumer Financial Protection Bureau (CFPB). *Id.*

105. Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank) § 111, 12 U.S.C. § 5321 (2018); CONG. RSCH. SERV., R44918, supra note 100 ("The financial regulatory system has been described as fragmented, with multiple overlapping regulators and a dual state-federal regulatory system.").

106. Cross, *supra* note 2.

107. *See* Exec. Order No. 14036, 86 Fed. Reg. 36987 (July 9, 2021) (https://www.whitehouse.gov/briefing-room/presidential-actions/2021/07/09/executive-order-on-promoting-competition-in-the-american-economy/) [https://perma.cc/7YBF-RNV4] (encouraging the CFPB to move forward with the proposed rulemaking under section 1033 of the Dodd-Frank); *see also* Consumer Access to Fin. Rec., 85 Fed. Reg. 71003 (proposed Nov. 6, 2020) (https://files.consumerfinance.gov/f/documents/cfpb_section-1033-dodd-frank_advance-notice-proposed-rulemaking_2020-10.pdf) [https://perma.cc/83K5-4Y5Q] (requesting that "interested parties" comment and these specific topics: benefits and costs of consumer data access, competitive incentives and authorized data access, standard-

Despite the lack of regulation from U.S. agencies, the market demand for Open Banking has prompted several major marketplace participants in the banking and financial services industry to partner with fintechs to meet consumer demands.[108] Most notably, Mastercard and Visa have recently acquired two major fintech companies with the hopes of staying relevant in the age of technology and innovation through the implementation of Open Banking technology.[109]

Large corporations, like Mastercard and Visa, are not the only entities responding to the consumer demand for Open Banking technology.[110] In September 2021, Live Oak Bank, a small business bank in Wilmington, North Carolina, finalized the conversion to Finxact, a fintech offering Open Banking API.[111] The general idea for Live Oak Bank's move to Open Banking technology is to make credit more accessible and timely for small businesses.[112] This access to credit can be extremely important, especially in the time of the COVID-19 global pandemic, for businesses that might not otherwise have the cash flow to stay afloat.

In response to this market push for Open Banking, President Joseph Biden has urged U.S. regulators, specifically the CFPB, to move forward with rulemaking that would "facilitate the portability" of financial data, enabling consumers to easily switch financial institutions and take advantage of "innovative financial products."[113] Biden's Executive Order on "Promoting Competition in the American Economy"

---

setting, access scope, consumer control and privacy, legal requirements other than section 1033, data security, and data accuracy).

108. *See* CARPENTER WELLINGTON PLLC, supra note 5 (announcing Visa and Mastercard's acquisition of fintech companies to implement Open Banking capabilities to meet consumer demands).

109. *Id.*

110. *See* Cross, *supra* note 2 (discussing Live Oak Bank's recent implementation of Open Banking technology).

111. *See Live Oak Bank Ushers in New Era of Open Banking*, PR NEWSWIRE (Sept. 7, 2021) https://www.prnewswire.com/news-releases/live-oak-bank-ushers-in-new-era-of-open-banking-301370346.html [https://perma.cc/BF2T-2AWM] (announcing Live Oak Bank's recent conversion to Finxact on September 7, 2021).

112. *See id.* ("By accessing its open APIs and extensible components, banks are able to invent, curate, and launch products at the speed required to meet customer expectations in today's marketplace.").

113. This Executive Order also addresses other areas of the American economy that could benefit from increased competition within the marketplace. Exec. Order No. 14036, 86 Fed. Reg. 36987 (July 9, 2021) https://www.whitehouse.gov/briefing-room/presidential-actions/2021/07/09/executive-order-on-promoting-competition-in-the-american-economy/ [https://perma.cc/7YBF-RNV4] (encouraging the CFPB to move forward with the proposed rulemaking under section 1033 of the Dodd-Frank).

addresses competition in various industries and points to consolidation in certain industries as the reason for lack of competition.[114] By promoting competition, especially within the financial services industry, steep and hidden fees attributed to industry consolidation may be eliminated, making credit and financial products more affordable.[115]

According to the 2021 FinHealth Spend Report, published by the Financial Health Network, a nonprofit research group, over $300 billion was spent on interest and fees for everyday financial services in 2020 alone.[116] Financially Coping and Vulnerable Households[117] paid $255 billion of the $300 billion interest and fees on short-term credit products,[118] long-term credit,[119] single payment credit,[120] and payments and accounts.[121] This data illustrates the growing financial gap in the U.S. and presents an opportunity for innovation and competition within the marketplace to close this gap.[122]

The Dodd-Frank Wall Street Reform and Consumer Protection Act ("Dodd-Frank") was enacted in part to address the kind of the

---

114. *Id.*

115. *See id.* ("In the financial-services sector, consumers pay steep and often hidden fees because of industry consolidation.").

116. FIN. HEALTH NETWORK, THE FINHEALTH SPEND REPORT, 5 (2021) https://s3.amazonaws.com/cfsi-innovation-files-2018/wp-content/uploads/2021/04/19180204/FinHealth_Spend_Report_2021.pdf [https://perma.cc/D9WW-8XZP].

117. *See id.* at 12 ("Approximately two-thirds of people in America are classified as Financially Coping (struggling with some aspects of their financial lives) or Vulnerable (struggling with almost all aspects of their financial lives).").

118. Short-term credit is credit products that function either on an installment basis with terms from a few months to two years or as a revolving line of credit (e.g., credit cards, installment loans, rent-to-own, title loans). *Id.*

119. Long-term credit is a loan that functions on an installment basis with a typical term of two years or more (e.g., auto leases, auto loans, and private student loans). *Id.*

120. Single payment credit is a loan that is due in one lump sum, typically with terms of one month of less (e.g., overdraft, pawn, payday, and refund anticipation checks). *Id.*

121. Payments and accounts are products that allow consumers to transact, convert, send, receive, deposit, invest and hold funds. Fees typically associated with this type of product are account maintenance fees, check cashing fees, and money order fees). *Id.*

122 . *See* FIN. HEALTH NETWORK, THE FINHEALTH SPEND REPORT, 5 (2021) https://s3.amazonaws.com/cfsi-innovation-files-2018/wp-content/uploads/2021/04/19180204/FinHealth_Spend_Report_2021.pdf [https://perma.cc/D9WW-8XZP] (exploring how many low-income communities are struggling financially and innovation in the marketplace might provide opportunities for economic advancement among these communities through new financial products and services).

consumer protection issues outlined in the FinHealth Spend Report.[123] Section 1011 of the act established the CFPB, granting the Bureau the power to "regulate the offering and provision of consumer financial products or services."[124] Dodd-Frank also empowered the CFPB to promulgate rules surrounding "consumer rights to access information" under Section 1033.[125] Section 1033, however, does not go into specifics for how financial institutions are supposed to make personal data available to consumers, and it does not specifically address the concept of Open Banking.[126]

While the CFPB has yet to enact any regulation surrounding Open Banking, the topic has been on its agenda since 2016.[127] In 2016, the CFPB issued a notice to request information regarding "consumer rights to access financial account and account-related data in usable electronic form."[128] After receiving feedback from this request in 2017, the Bureau developed a set of "Consumer Protection Principles" for market participants to consider when implementing Open Banking technology.[129] These guidelines considered the following subject categories: (1) access; (2) data scope and usability; (3) control and informed consent; (4) authorizing payments; (5) security; (6) transparency of access; (7) accuracy; (8) ability to dispute and resolve unauthorized access; and (9) efficient and effective accountability mechanisms.[130]

---

123. The Dodd-Frank Wall Street Reform and Consumer Protection Act was enacted in response to the financial crisis of 2008, recognizing the "broken financial regulatory system" that caused the crisis. *See Wall Street: The Dodd-Frank Act*, OBAMA WHITE HOUSE, https://obamawhitehouse.archives.gov/economy/middle-class/dodd-frank-wall-street-reform [https://perma.cc/QRE2-PPTQ].

124. Dodd-Frank Wall Street Reform and Consumer Protection Act, Pub. L. No. 111-203, § 929-Z, 124 Stat. 1376, 1871 (2010) (codified at 15 U.S.C. § 780) https://www.cftc.gov/sites/default/files/idc/groups/public/@swaps/documents/file/hr4173_enrolledbill.pdf [https://perma.cc/T225-33MK].

125. *Id.*

126. *See* Shakeel Hasim, *America Might Finally Get Open Banking – But Not Without a Fight*, PROTOCOL (Oct. 27, 2020), https://www.protocol.com/open-banking-dodd-frank-data-fintech [https://perma.cc/ZA86-UR4C] ("[T]here are indications that some emerging market practices may not reflect the access rights described in Section 1033.").

127. Consumer Access to Fin. Rec., 81 Fed. Reg. 83806 (Nov. 22, 2016) (to be codified at 12 U.S.C. 5511(c); 12 U.S.C. 5512(c)) https://www.govinfo.gov/content/pkg/FR-2016-11-22/pdf/2016-28086.pdf [https://perma.cc/KD62-X2WZ].

128. *Id.*

129. *See* CONSUMER FIN. PROT. BUREAU, *supra* note 98, at 1.

130. *Id.* at 3-4.

The feedback solicited by the CFPB addressed many of the previously mentioned concerns surrounding data sharing technology such as accountability within a transaction, data security, and who controls the data being shared.[131] However, the CFPB's guidelines are just that — guidelines—and are in no way binding on financial institutions or the fintechs they share consumer data with.[132] Furthermore, the CFPB itself recognized that guidelines might not be enough to protect consumers in the developing market of data sharing.[133]

In February of 2020, the CFPB held a symposium featuring a panel of industry experts speaking on the potential risk and benefits of Open Banking.[134] The CFPB followed with an Advanced Notice of Proposed Rulemaking ("ANPR") in October 2020.[135] The purpose of both the symposium and the ANPR was to solicit comments and information to assist the Bureau in developing regulations for Open Banking under the Section 1033 of the Dodd-Frank Act.[136] Some of the main issues the CFPB is hoping to address with the proposed regulations are data security, consumer control over their data, and how this regulation would interact with other regulatory agencies who might have jurisdiction.[137] However, the proposed regulations are still under advisement with little prospect of major changes any time soon.[138]

---

131. *Id.* at 1.

132. *See id.* at 2-3 ("These stakeholders generally take the view that CFPB regulatory action, which could include a rulemaking that involves Section 1033 of the Dodd-Frank Act, clarification of existing regulations, or expanding CFPB supervisory authority to include aggregators and account data users by means of 'larger participant' rulemakings, may be necessary to ensure consumers are protected as the market continues to develop.").

133. *Id.*

134. *See CFPB Symposium: Consumer Access to Financial Records*, CONSUMER FIN. PROT. BUREAU (Feb. 26, 2020), https://files.consumerfinance.gov/f/documents/cfpb_agenda_symposium-consumer-access-financial-records.pdf [https://perma.cc/9HFM-65SH] (providing the agenda to the CFPB's most recent symposium regarding Open Banking regulation).

135. Consumer Access to Fin. Rec., 85 Fed. Reg. 71003 (proposed Nov. 6, 2020), https://files.consumerfinance.gov/f/documents/cfpb_section-1033-dodd-frank_advance-notice-proposed-rulemaking_2020-10.pdf) [https://perma.cc/83K5-4Y5Q].

136. *Id.*

137. *See id.* (requesting that "interested parties" comment and these specific topics: benefits and costs of consumer data access, competitive incentives and authorized data access, standard-setting, access scope, consumer control and privacy, legal requirements other than section 1033, data security, and data accuracy).

138. As of the date of this Note, the CFPB has yet to provide any further updates on the ANPR.

One potential obstacle to the proposed regulation is it is unclear how far the CFPB's potential rulemaking will reach.[139] Section 1011 of the Dodd-Frank Act explicitly grants the CFPB the power to "regulate the offering and provision of consumer financial products or services."[140] Additionally, section 1033 of the Act requires "covered persons" to follow regulation enacted by the CFPB to "make available to a consumer . . . information in the control or possession of the covered person concerning the consumer financial product or service that the consumer obtained from such covered person."[141] However, it is not explicitly clear if this power will extend to third-party service providers.[142]

The Dodd-Frank Act defines "consumer financial product or service" as "any financial product or service that . . . is offered or provided for use by consumers primarily for personal, family, or household purposes" or "provided in connection with a consumer financial product or service."[143] The Act defines "covered persons" of the CFPB's regulation as "any person that engages in offering or providing a consumer financial product or service."[144] An affiliate of such person may also be a "covered person" if the affiliate provides a service to the financial services provider.[145] Based on these defined terms, it appears that the CFPB might have the ability to regulate any entity involved in a

139. *See* CONSUMER FIN. PROT. BUREAU, *supra* note 98, at 2-3 ("These stakeholders generally take the view that CFPB regulatory action, which could include a rulemaking that involves Section 1033 of the Dodd-Frank Act, clarification of existing regulations, or expanding CFPB supervisory authority to include aggregators and account data users by means of 'larger participant' rulemakings, may be necessary to ensure consumers are protected as the market continues to develop.").

140. Dodd-Frank Wall Street Reform and Consumer Protection Act, Pub. L. No. 111-203, § 929-Z, 124 Stat. 1376, 1871 (2010) (codified at 15 U.S.C. § 78o) https://www.cftc.gov/sites/default/files/idc/groups/public/@swaps/documents/file/hr4173_enrolledbill.pdf [https://perma.cc/T225-33MK].

141. *Id.*

142. *See* CONSUMER FIN. PROT. BUREAU, *supra* note 98, at 2-3 ("These stakeholders generally take the view that CFPB regulatory action, which could include a rulemaking that involves Section 1033 of the Dodd-Frank Act, clarification of existing regulations, or expanding CFPB supervisory authority to include aggregators and account data users by means of 'larger participant' rulemakings, may be necessary to ensure consumers are protected as the market continues to develop.").

143. Dodd-Frank Wall Street Reform and Consumer Protection Act, Pub. L. No. 111-203, § 929-Z, 124 Stat. 1376, 1871 (2010) (codified at 15 U.S.C. § 78o) https://www.cftc.gov/sites/default/files/idc/groups/public/@swaps/documents/file/hr4173_enrolledbill.pdf [https://perma.cc/T225-33MK].

144. *Id.*

145. *See id.* ("The term 'covered person' means— (A) any person that engages in offering or providing a consumer financial product or service; and (B) any affiliate of a person described in subparagraph (A) if such affiliate acts as a service provider to such person.").

financial services transaction.[146] Stakeholders responding to the CFPB's initial request for information also believe that the Bureau has jurisdiction over these third-party players.[147]

Some comments from the CFPB's guidelines appear to question whether the Bureau has the jurisdictional reach to regulate every entity involved in an Open Banking transaction.[148] More specifically, the CFPB questions whether its "supervisory authority" would need to be expanded to "include aggregators and account data users."[149] Therefore, while it appears the CFPB's has a broad reach to regulate much of an Open Banking transaction, its current power under the Dodd-Frank Act might fall short of effectively regulating every participant within these transactions.[150] Without the ability to regulate every entity involved in a transaction, any proposed regulation might not be as effective it would be otherwise.

In the absence of Open Banking regulation from U.S. agencies, private-sector actors have ventured to fill the void.[151] The Financial Data Exchange, a large advocacy group of prominent U.S. and Canadian financial institutions, is pushing for the adoption of an industry-wide API standard.[152] Among this group are financial institutions, fintechs, and financial data aggregators, all of whom recognize the demand consumers have for Open Banking technology.[153] However, this group also recognizes the need for a secure and transparent way to share consumer data.[154]

---

146. *See* CONSUMER FIN. PROT. BUREAU, *supra* note 98, at 8 ("Relatedly, consumer advocates tell the Bureau that they believe the Bureau has regulatory and enforcement jurisdiction over aggregators and account data users.").

147. *Id.*

148. *See id.* at 3 ("These stakeholders generally take the view that CFPB regulatory action, which could include a rulemaking that involves Section 1033 of the Dodd-Frank Act, clarification of existing regulations, or expanding CFPB supervisory authority to include aggregators and account data users by means of 'larger participant' rulemakings, may be necessary to ensure consumers are protected as the market continues to develop.").

149. *Id.*

150. *Id.*

151. Tom Auchterlonie, *US Open-Banking Regulation Gets Biden's Backing*, EMARKETER (July 13, 2021), https://www.emarketer.com/content/us-open-banking-regulation-gets-biden-s-backing [https://perma.cc/4Y8W-FAFT].

152. *Id.*

153. *See* Cross, *supra* note 2 (explaining that the members of the financial-services sector recognized that consumers really wanted to use Open Banking technology, but also recognized that the industry needs to figure out a way to make sure this can be done safely and transparently).

154. *Id.*

In a press release from December of 2020, the Financial Data Exchange announced new open finance standards[155] and updates to the API technology.[156] This latest version of data sharing technology includes new features reported to improve data security and data quality, to further the organization's goal of unifying the financial industry through secure, and standardized methods of data sharing.[157] While the CFPB and private-sector actors such as the Financial Data Exchange are attempting to fill the regulatory gap with informal guidance, it is important to remember that this guidance is not binding on any institution.[158] Institutions within the financial services sector are left to their own devices to remain in compliance with the many agencies who govern financial transactions and data sharing.[159]

IV. HOW OPEN BANKING TECHNOLOGY AFFECTS CONSUMER DATA

A. Data Security

The U.S. is no stranger to large-scale cyberattacks.[160] Hackers are becoming increasingly more sophisticated, and many recent attacks have paralyzed large companies, compromising millions of consumers' sensitive data.[161] According to Verizon's Data Breach Investigations Report, there were 5,258 confirmed data breaches in the U.S. in 2020

155. *See Financial Data Exchange Releases New Open Finance Standards & FDX API Version 4.5*, FIN. DATA EXCH., (Dec. 8, 2020) https://financialdataexchange.org/FDX/News/Press-Releases/FDX_Launches_Open_Finance_Standards_And_FDX_API_4.5.aspx [https://perma.cc/24TT-5S9T] ("These new standards provide guidance to both industry stakeholders and regulators to better understand the technology used in the data sharing marketplace, and how to better protect and share consumer data.").

156. *Id.*

157. *Id.*

158. *See* Egan, *supra* note 3 ("In October 2017, the CFPB released the 'Consumer Protection Principles' for participants in the developing market for services based on the consumer-authorized use of financial data. According to the CFPB, the principles are not legally binding rules.").

159. *See* CONG. RSCH. SERV., R44918, *supra* note 100 ("The financial regulatory system has been described as fragmented, with multiple overlapping regulators and a dual state-federal regulatory system.").

160. *See Hackers Steal $600m in Major Cryptocurrency Heist*, *supra* note 19 (reporting on the recent Bitcoin heist); *see also* Crosman, *supra* note 19 (reporting on recent attacks on three small, unnamed banks); *see also* Rotenberg, *supra* note 19 (reporting on the recent Capital One data breach and how Congress needs to act to prevent future attacks).

161. *See* Rotenberg, *supra* note 19 (reporting on the recent Capital One breach that compromised millions of customers sensitive data); *see also Hackers Steal $600m in Major Cryptocurrency Heist*, *supra* note 19 (reporting on the recent Bitcoin heist).

alone.[162] Financial gain was the most common motivation for these attacks,[163] and web applications were the main attack vector.[164]

One of the largest breaches of personal data held by a financial institution in U.S. history, the 2019 Capital One cyber-attack,[165] impacted 106 million customers.[166] Through this breach, hackers obtained personal information—including social security numbers, bank account numbers, names, and home addresses—of Capital One customers.[167] In the aftermath of this attack, Capital One was fined $80 million by the OCC and ordered by both the OCC and Federal Reserve to "overhaul its operations" to guard against any future attacks.[168]

On August 10, 2021, hackers exploited a vulnerability in Poly Network's system[169] and stole over 600 million dollars of cryptocurrency.[170] Poly Network, a crypto currency platform, facilitates peer-to-peer transactions and allows users to transfer or swap tokens across different blockchains.[171] This recent attack of Poly Network's platform was one of the biggest attacks, in terms of dollar amounts, in decentralized finance history.[172]

---

162. VERIZON BUS., 2021 DATA BREACH INVESTIGATIONS REPORT (2021), at 6 https://enterprise.verizon.com/resources/reports/2021-data-breach-investigations-report.pdf?_ga=2.112156807.2046190888.1631377396-20239801.1631377396&_gac=1.262950526.1631377396.CjwKCAjwp_GJBhBmEiwALWBQk0q-qyjg6EpS03VPRbDoTtAchF9bWgNxtllLDJCrNhCjzZTDkpq79hoCQU4QAvD_BwE [https://perma.cc/Q63D-CH6N].

163. *See id.* at 12-13 (estimating over 75% of data breaches are financially motivated, remaining the most common type of attack).

164. *Id.*

165. Rotenberg, *supra* note 19.

166. *Id.*

167. *Id.*

168. *See* Pete Schroeder, *Capital One to Pay $80 Million Fine After Data Breach*, REUTERS (Aug. 6, 2020, 11:57 AM), https://www.reuters.com/article/us-usa-banks-capital-one-fin/capital-one-to-pay-80-million-fine-after-data-breach-idUSKCN2522DA [https://perma.cc/SBF8-4XUM] ("The fine, announced Thursday by the Office of the Comptroller of the Currency, punishes the bank for failing to adequately identify and manage risk as it moved significant portions of its technological operations to the cloud.").

169. *See* John, *supra* note 169 ("A lesser-known name in the world of crypto, Poly Network is a decentralized finance (DeFi) platform that facilitates peer-to-peer transactions with a focus on allowing users to transfer or swap tokens across different blockchains.").

170. *Hackers Steal $600m in Major Cryptocurrency Heist*, *supra* note 19.

171. *See* John, *supra* note 169 ("A lesser-known name in the world of crypto, Poly Network is a decentralized finance (DeFi) platform that facilitates peer-to-peer transactions with a focus on allowing users to transfer or swap tokens across different blockchains.").

172. *Hackers Steal $600m in Major Cryptocurrency Heist*, *supra* note 19 (Poly Network sent a letter to the hacker stating, "the amount of money you have hacked is one of the biggest in defi history.").

Unfortunately, cyber security analysts predict that data security problems, and breaches of this scale, will only get worse and more frequent.[173] Cybersecurity Ventures, the world's leading research firm on the global cyber economy, predicts that by 2025 cybercrime will cost the world $10.5 trillion annually by 2025.[174] In the face of these staggering figures, businesses—especially small businesses—cannot compete.[175] According to a Better Business Bureau survey, over 55% of small businesses lack the resources and knowledge to develop a cyber security plan to protect against cyberattacks.[176]

Despite the staggering number of consumers impacted by data breaches, consumers and institutions lack the proper tools to combat the attacks and assign liability as there is no comprehensive law in the U.S. which governs data protection.[177] Furthermore, there is no comprehensive federal law regulating how data is collected, shared, and stored.[178] Instead, there is a patchwork of federal regulation[179] and state law attempting to protect consumer data.

---

173. *See* Rotenberg, *supra* note 19 ("We urged Congress to updated federal privacy laws and to establish a data protection agency to address growing consumer concern about the misuse of their personal data.").

174. Steve Morgan, *Cybercrime to Cost the World $10.5 Trillion Annually by 2025*, CYBERSECURITY VENTURES (Nov. 13, 2020), https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/ [https://perma.cc/8CLE-EUDM].

175. *See id.* (explaining that more than half of cyberattacks are committed against small-to-midsized businesses who lack the knowledge and resources to protect themselves and that 60% of these attacks result in the affected business going out of business).

176. *Id.*

177. It is important to contrast the U.S.'s current model for regulating data protection with the uniform way in which the EU regulates their data protection. *Compare* Angelique Carson, *Data Privacy Laws: What You Need to Know in 2021*, OSANO (July 20, 2021), https://www.osano.com/articles/data-privacy-laws [https://perma.cc/DU98-JNQV] (providing an overview of all the different agencies who govern consumer data protection), *with* Wolford, *supra* note 71 (explaining the how the EU's uniform regulation of data security works).

178. Angelique Carson, *Data Privacy Laws: What You Need to Know in 2021*, OSANO (July 20, 2021) https://www.osano.com/articles/data-privacy-laws [https://perma.cc/DU98-JNQV]; *see also* Thorin Klosowski, *The State of Consumer Data Privacy Laws in the US (And Why it Matters)*, N.Y. TIMES, (Sept. 6, 2021) https://www.nytimes.com/wirecutter/blog/state-of-privacy-laws-in-us/ [https://perma.cc/QC7Y-GEU7] (explaining the different federal and state regulation of data privacy).

179. *See* Thorin Klosowski, *The State of Consumer Data Privacy Laws in the US (And Why it Matters)*, N.Y. TIMES, (Sept. 6, 2021) https://www.nytimes.com/wirecutter/blog/state-of-privacy-laws-in-us/ [https://perma.cc/QC7Y-GEU7] ("The United States doesn't have a singular law that covers the privacy of all types of data. Instead, it has a mix of laws that go by acronyms like HIPPA, FCRA, FERPA, GLBA, ECPA, COPPA, and VPPA.").

Most of the federal regulations either deal only with very specific transactions or are antiquated due to technological advances.[180] For example, the Federal Trade Commission Act ("FTC Act") only authorizes the FTC to penalize an app or website that violates its own privacy policy while the outdated Video Privacy Protection Act ("VPPA") merely prevents the disclosure of VHS cassette tape rental records.[181] This federal patchwork of regulation leaves several critical gaps in data protection, including: (1) no requirement that companies notify consumers in the event their data is compromised in a breach; and (2) no law prohibiting third parties from selling consumer data without that consumer's consent.[182]

A few states have enacted their own comprehensive data protection law to protect their citizens.[183] As of March, 2022, California, Virginia, and Colorado, were the only states that have comprehensive consumer privacy laws.[184] Four other states—Massachusetts, New York, North Carolina, and Pennsylvania—have consumer data proposals that have been assigned to a committee for study.[185] Each state's laws vary, making it difficult for consumers to know their rights surrounding certain data protection and privacy issues.[186] Too much variation among state laws also creates confusion for companies who do business with citizens of multiple states.[187] Not only do such companies have to ensure that they are meeting the federal requirements from the patchwork of agencies, but they must also ensure they are in compliance with each individual state's laws.[188] With the increase in cyber-attacks and data protection issues, this "patchwork" of regulation does not cut it anymore.[189] Instead, the U.S.

180. *Id.*
181. *Id.*
182. *Id.*
183. *Id.*
184. *Id.*
185. Klosowski, *supra* note 179.
186. *See id.* (There's also a risk of too many state laws generating confusion, both operationally for companies and practically for consumers. Whitney Merrill, a privacy attorney and data protection officer, said that a federal law would make matters easier for everyone).
187. *Id.*
188. *Id.*
189. *See* Rotenberg, *supra* note 19 (explaining how federal privacy laws and a data protection agency are needed to combat the growing issue of data security and protection).

needs a federal agency to protect consumer data and establish a baseline that will raise data protection standards.[190]

With the move towards Open Banking technology, data security is one of the main concerns.[191] Currently, there is no set standard or regulatory structure that governs the security of APIs that enable data sharing.[192] Even worse, many applications still use "outmoded and insecure two-[f]actor authentication in the form of SMS or email to verify transactions," making it easy for hackers to intercept sensitive consumer data.[193] Several documented breaches have resulted from flawed API technology and lack of proper security measures.[194]

According to the Identity Theft Resource Center, API use was up 61% in 2020, with API attacks up by 211% and contributing to some of the biggest security breaches in 2020 and 2021.[195] While some companies may take initiative on their own to implement greater security measures, this will not solve the problem of subpar APIs entirely.[196] When data is being shared across multiple platforms, with multiple entities, financial institutions lose control over how that data is handled or protected once it is transmitted.[197] Non-banking industries that might receive consumer data in an Open Banking system may not share the same heightened level of security that regulated banks do.[198] Ultimately, if just one entity in the data sharing transaction has subpar security measures, consumer data remains at risk.[199]

---

190. *See The State of Consumer Data Privacy Laws in the US (And Why it Matters)*, *supra* note 179 ("There's also a risk of too many state laws generating confusion, both operationally for companies and practically for consumers. Whitney Merrill, a privacy attorney and data protection officer, said that a federal law would make matters easier for everyone.").

191. *See* Saavedra-Lim, *supra* note 21 (providing an overview of the risks associated with Open Banking technology); *see also* Johnson, *supra* note 20 ("The biggest danger for the banks is they have provided the service as agreed with the regulator, but once beyond their walls, privacy and security can go awry.").

192. Egan, *supra* note 3.

193. Johnson, *supra* note 20.

194. *See API Attacks Become More Common as Software Grows in Popularity*, *supra* note 46 (explaining that Facebook, LinkedIn, Peloton and Microsoft all experienced data breaches that were the result of flawed API technology).

195. *Id.*

196. *See* Saavedra-Lim, *supra* note 21 (explaining that if just one "player" in the Open Banking transaction does not have the proper security measures the whole transaction is vulnerable).

197. *Id.*

198. *Id.*

199. *Id.*

While organizations like the Identity Theft Resource Center have issued some guidance on how to better utilize API technology safely, there is no direct regulation surrounding the development of this technology in the U.S.[200] This lack of regulation surrounding relatively new technology stands in stark contrast to the EU's strict guidelines for data sharing.[201]

With several entities handling consumer data in a single transaction, the question is then who would be held accountable in the event of a data breach in which consumer data is compromised.[202] For example, if a financial institution collects data from the consumer, does the financial institution own this data and is it therefore responsible in the event of a subsequent breach by one of its technology partners?[203] Is the consumer responsible for the risks associated with sharing their data? Is this risk something that can be contracted around? There are no clear answers to these questions under the current Open Banking structure in the U.S.[204]

This uncertainty and lack of accountability is not only a detriment to the consumer, but it also makes implementing Open Banking expensive for those trying to enter the Open Banking market.[205] Without the ability to gauge the liability risk of a new partnership in the Open Banking marketplace, institutions might be weary to implement new technology with known security risks.[206] The EU addressed this uncertainty in the marketplace by standardizing the technology used to share data under PSD2 and providing institutions with clear guidelines for data sharing practices through the GDPR.[207]

---

200. *See API Attacks Become More Common as Software Grows in Popularity*, *supra* note 46 (encouraging businesses utilizing API technology to implement strong testing protocols and security to ensure that consumer data is protected from cybercriminals).

201. *See* Wolford, *supra* note 71 (self-proclaiming that the GDRP is the "toughest privacy and security law in the world").

202. *See* Saavedra-Lim, *supra* note 21 (raising the question of which "player" in an Open Banking transaction would be responsible in the event of a data breach).

203. *See id.* (raising the question of which "player in an Open Banking transaction would be responsible in the event of a data breach).

204. *Id.*

205. *See id.* (explaining the benefits of standardized regulation and how the U.S. will have to "establish robust data management" strategies and thoughtfully onboard new partners, which can be resource intensive).

206. *Id.*

207. *Id.*

B. Data Ownership

Data security is not the only risk with sharing sensitive financial data.[208] Who actually owns the data being transmitted between consumers and third parties is a big question that remains unanswered in the U.S.[209] While the basic principle of data sharing is that consumers own their data, both legal and policy issues make it difficult to apply this principle in the financial sector.[210] The main issue is what exactly qualifies as consumer data.[211] Take, for example, the Experian Boost technology which allows consumers to increase their credit score.[212] While the social security number and other personal information input into the system is pretty clearly the consumer's, is the data produced by Experian's technology owned by the consumer or Experian?[213]

It is even less clear what happens when data is shared across industries.[214] For example, which regulations will apply when the healthcare industry and the financial industry share data?[215] Will HIPPA regulations apply or will bank regulations apply?[216] Whose document retention policies will be followed?[217] These questions create significant legal uncertainty for all parties involved in a transaction.[218] This, again, prevents small players who do not have a lot of resources from entering the market, further consolidating the financial services industry.[219]

---

208. Egan, *supra* note 3.

209. *See* Fracassi & Magnuson, *supra* note 99, at 347 ("The Financial Data and Technology association, an industry consortium, has similarly argued that 'the right for the consumer to control their data…is murky.'").

210. *Id.*

211. *See id.* (raising the issues of when consumer data becomes vendor data when using proprietary vendor technology).

212. *Id.*

213. *Id.*

214. *See* Saavedra-Lim, *supra* note 21 ("Aside from security issues, there must be consideration for what happens when data is shared across industries – for example, retail, healthcare and others – come together.").

215. *Id.*

216. *Id.*

217. *Id.*

218. *See id*. ("These are unprecedented new challenges stemming from data, ironically the same data that gives life to Open Banking.").

219. *See* Kosoff, *supra* note 22 (explaining that PSD2 is more friendly to fintech companies as it "streamlines access to a growing network of bank data," as opposed to fintechs in the U.S. having to create individual data sharing agreements with each bank partner which can be resource intensive).

V. THE FUTURE OF OPEN BANKING IN THE U.S.

Implementing uniform Open Banking and data protection regulations in the U.S. will benefit consumers and the industry as a whole in two major ways: (1) by promoting competition within the market, making credit and financial products more affordable for the consumer; and (2) by giving consumers control of their data and making the practice of data sharing safer.[220]

First, uniform federal regulation will likely promote competition within the market.[221] While moving towards a more technologically innovative marketplace might leave some smaller banks in the dust, this could be avoided if U.S. regulators require the development of API technology and provide for its framework.[222] As it stands now, it is extremely expensive for smaller banks and fintechs to implement Open Banking technology due to the legal uncertainty.[223] Not only do these companies have to meet the requirements of all the different federal agencies that govern data sharing, but also ensure that the many different state law requirements have been met.[224]

This legal uncertainty surrounding Open Banking and data sharing transactions requires a great deal of resources to partner with a new bank or application.[225] While major participants in the financial industry have proven to have the resources to enter the Open Banking

220. The EU replaced outdated authentication factors with a new two-factor authentication. *See* Gaynor, *supra* note 54 (explaining that the new way to authenticate consumer identity prevents payment fraud and makes data sharing more secure).

221. Competition was a major theme throughout the PSD2 directive. *See* Council Directive, 2015/2366, art. 82(1)(c), 2015 O.J. (L 337) 58 (EU) https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015L2366 [https://perma.cc/3GA3-K7LC] (outlining several measures to ensure that healthy competition remains in the financial services sector).

222. As discussed previously, if regulation does not push the U.S. towards an Open Banking model, the market will. While some small banks might not be able to keep up with the technology demands of Open Banking, uniform regulations will at least level the playing field some and allow smaller banks who might already have superior technology in place enter the Open Banking arena by eliminating the need for a lot of legal resources to ensure they are in compliance with all of the current patchwork regulation.

223. *See* Kosoff, *supra* note 22 (explaining that all banks must continue to abide by existing regulation such as consumer protection and privacy laws).

224. *See* Klosowski, *supra* note 179 ("There's also a risk of too many state laws generating confusion, both operationally for companies and practically for consumers. Whitney Merrill, a privacy attorney and data protection officer, said that a federal law would make matters easier for everyone.").

225. *See* Kosoff, *supra* note 22 (explaining that PSD2 is more friendly to fintech companies as it "streamlines access to a growing network of bank data," as opposed to fintechs in the U.S. having to create individual data sharing agreements with each bank partner which can be resource intensive).

market,[226] many of the smaller banks will likely fall by the wayside, further consolidating the market.

Moreover, the U.S. is quickly moving towards the Open Banking market regardless of whether or not it is regulated.[227] The market demand for Open Banking technology leaves little choice to financial services providers,[228] and without standardized rules, the U.S. may lose out to European companies.[229] Developers prefer the certainty of a uniformly regulated market, as opposed to the uncertainty and large liability risk in the U.S. market.[230] Instead of navigating the patchwork of regulation of the U.S. marketplace, developers will be better suited to innovate in an environment with less legal uncertainty.[231] This is only further complicated when data is being shared across industries.[232]

The EU faced a similar dilemma with cross-border payments and the question of which country's laws would govern cross-border transactions, creating, in a sense, a fragmented regulatory system.[233] To face this regulatory uncertainty, the EU enacted uniform regulations instead of relying on multiple regulatory bodies to govern one transaction.[234] The U.S. already has a good foundation to enact uniform regulation through the CFPB. While input from major agencies within the financial regulatory system would be necessary to successfully regulate the Open Banking market, the CFPB could use its authority under the Dodd-Frank Act to touch providers that might not necessarily be under the reach of other financial regulators.[235]

---

226. *See* Carpenter Wellington, PLLC, supra note 5 (reporting on Mastercard and Visa's recent acquisition on fintech companies to enter the Open Banking market).

227. *See* Cross, *supra* note 2 (discussing the consumer demand for Open Banking technology and how this demand will push the industry towards the Open Banking market).

228. *Id.*

229. *See* Kosoff, *supra* note 22 (discussing that developers may potentially move business to the EU due to the standardization of the market).

230. *Id.*; *see also* Klosowski, *supra* note 179 (explaining the patchwork of different federal and state regulations governing consumer data privacy in the U.S.).

231. Kosoff, *supra* note 22.

232. Johnson, *supra* note 20.

233. *See* Katherine E. Ruiz Díaz, *Pre-Paid Payment Cards in A Post*-Schrems *World: A Case Study on the Effects of the Privacy Shield Principles*, 9 U.P.R. BUS. L.J. 86, 101 (2018) (explaining that PSD2 provided the legal framework for the EU to implement a single market for payments, achieving the goal of enabling easy and secure national payments).

234. *Id.*

235. *See* CONG. RSCH. SERV. R44918, *supra* note 100, at 23 (describing the role of the FSCO and its authority to facilitate "information sharing and coordination amount financial regulators").

However, it is currently unclear whether the CFPB has the power to regulate every entity involved in an Open Banking transaction.[236] When contemplating new regulation, the CFPB should be unambiguous as to whom the regulation applies, and Congress should consider expanding the CFPB's authority to effectively regulate all participants within an Open Banking transaction.[237] Otherwise, there may be critical gaps in consumer protection.

Regardless of whether the U.S. uniformly regulates the Open Banking market, there is still much to be desired in terms of data protection and security.[238] Current methods of authentication are outmoded and leave consumers and financial institutions vulnerable to sophisticated attacks.[239] While the patchwork of agency regulation may have sufficed in the past, the advancement of technology and sophisticated cyber criminals require a revamp of current data regulation.[240]

Creating an agency that is solely responsible for the collection, sharing, and storage of data would provide an opportunity to raise the standard for data protection.[241] Each individual agency could pursue and penalize offenders, but would have to work from the framework provided by the agency responsible for data regulation. This model would mimic the EU's current model where individual countries within the EU work within the same framework and regulatory model but handle the offenders of the GDPR at the individual level.[242]

It is important, however, to understand that the EU's uniformly regulated market is still in its infancy and there is very little data on how the PSD2 and the GDPR have positively affected the financial

236. *See* CONSUMER FIN. PROT. BUREAU, *supra* note 98, at 2-3 ("These stakeholders generally take the view that CFPB regulatory action, which could include a rulemaking that involves Section 1033 of the Dodd-Frank Act, clarification of existing regulations, or expanding CFPB supervisory authority to include aggregators and account data users by means of 'larger participant' rulemakings, may be necessary to ensure consumers are protected as the market continues to develop.").

237. *Id.*

238. *See* Rotenberg, *supra* note 19 (advocating for federal privacy laws and a data protection agency to combat the growing issue of data security and protection).

239. Johnson, *supra* note 20.

240. *Id.*

241. *Id.*

242. *See Three Years of GDPR: The Biggest Fines So Far*, *supra* note 80 (explaining that each country's regulators handled the imposition of fines for each company).

marketplace and consumer as a whole.[243] However, the EU's move to a uniformly regulated marketplace has sparked a discussion, both at the federal level[244] and within the private sector, about the state of current legislation in the U.S. surrounding data protection, data sharing, and competition within the marketplace.[245] The CFPB recognizes that the Open Banking market is a quickly developing one, and that the current regulatory framework leaves both market participants and consumers vulnerable to legal uncertainty and technology flaws.[246]

It would also be prudent for the U.S. to impose harsh fines on those who violate any enacted Open Banking regulations.[247] Compliance with updated data security laws or Open Banking regulations is likely to be expensive for companies;[248] many companies may have to revamp their entire way of doing business.[249] To ensure that any enacted regulation is complied with and that consumers and other entities within an open transaction are protected, steep penalties have to be imposed on offenders who do not comply.[250] Otherwise, it may be cheaper not to comply than it would be to comply.

However, even though compliance with new regulation will likely be expensive, U.S. financial companies may benefit from stable,

---

243. There is actually data to the contrary, that data security issues are rising within the EU. *See* Justin Baltrusaitis, *GDPR Fines in Q3 Almost Hit €1 Billion, 20x More Than in Q1 and Q2 Combined,* FINBOLD (Oct. 7, 2021), https://finbold.com/gdpr-fines-q3-2021/ [https://perma.cc/X6HN-5KWH] ("According to data compiled by Finbold, the EU GDPR fines for 2021 Q3 hit €984.47 million, which is almost 20 times higher than cumulative fines of €50.26 million imposed during Q1 and Q2. To put this into perspective, the Q3 2021 GDPR fines are also three times higher than the €306.3 million imposed across the entire 2020.").

244. *See* CONSUMER FIN. PROT. BUREAU, *supra* note 98, at 2-3; Consumer Access to Financial Records, 85 Fed. Reg. 71003 (proposed Nov. 2, 2021).

245. *Financial Data Exchange Releases New Open Finance Standards & FDX API Version 4.5*, *supra* note 155.

246. *See* CONSUMER FIN. PROT. BUREAU, *supra* note 98, at 7-8.

247. You may remember the case taught in many first-year torts classrooms where punitive damages were awarded purely to ensure that it was not cheaper for the defendant to keep driving the mobile home through the plaintiff's property than to comply with trespass law. *See* Jacque v. Steenberg Homes, Inc., 563 N.W.2d 154 (Wis. 1997).

248. *See* Kosoff, *supra* note 22 (explaining that without standardization in Open Banking, fintechs must create "individual data sharing agreements," which can be resource intensive).

249. *Id.*

250. Both penalties and compensatory damages may be imposed on offenders under the GDRP requirements. *See* Wolford, *supra* note 71.

uniform regulations designed to protect consumer data.[251] Added consumer protection may be a selling point for some companies, especially in the midst of major data breaches.[252] This paradox will need to be addressed by the CFPB when considering new regulation; ensuring consumers are protected without unduly interfering with the free market.

VI. CONCLUSION

There is no question that the market, both nationwide and globally, has pushed the U.S. financial services industry towards an Open Banking platform.[253] In response to this push, government agencies have been slow to implement the regulations needed to keep consumer data safe.[254] With this lack of regulation comes the lack of accountability, and potential risks for consumers sharing their sensitive information, namely the risk of this data ending up in the hands of cybercriminals.[255]

While the U.S. has taken small steps towards regulating Open Banking technology, it is not enough. U.S. regulators need to take a page out of the EU's playbook and implement uniform regulations around Open Banking technology and cybersecurity. In order to do this, Congress needs to act and expand the CFPB's reach under the Dodd-Frank Act so that the Bureau not only has the authority to regulate the financial services market participants, but also the third-party servicers involved in a data sharing transaction. Without such regulation, there is an increased risk of further consolidation of the financial services market, an increase in security issues, and the potential for U.S. companies to lose business to EU rivals.

---

251. *See* Kosoff, *supra* note 22 (warning that the U.S. should take notice of PSD2 because standardization of Open Banking could give the European banking system a competitive edge).

252. *Hackers Steal $600m in Major Cryptocurrency Heist*, *supra* note 19; Rotenberg, *supra* note 19; Schroeder, *supra* note 168.

253. *See* Cross, *supra* note 2 (explaining how market demand is moving the U.S. towards an Open Banking market); Joy Macknight, *US and Canada Join the Open Banking Wave*, BANKER (Aug. 17, 2021, 10:26 AM), https://www.thebanker.com/Editor-s-Blog/US-and-Canada-join-the-open-banking-wave [https://perma.cc/86CE-33LA] (discussing recent developments in the U.S. and Canada in the realm of Open Banking technology and regulation).

254. *See* Cross, *supra* note 2 (discussing the lack of regulation of Open Banking technology in the U.S.).

255. Johnson, *supra* note 20.

SARA C. MARKOV*

* A huge thank you to my editors, Professor Broome, and my fellow staff members for your support and guidance throughout this writing process. And to my husband, Alex, thank you for your constant support and love. You helped make my dream of going back to school a reality, and for that, I am forever grateful.