Fair Credit Reporting Act and Financial Privacy Update—2019

*By Andrew Soukup, David A. Stein, and Lucille C. Bartholomew**

Introduction

The previous *Annual Survey*[1] shifted its focus from developments at the Consumer Financial Protection Bureau ("CFPB") that had pervaded earlier *Surveys*[2] to Congress, New York regulators, and the California legislature. This past year, federal agencies stepped back into the forefront by bringing high-profile enforcement actions and releasing a proposal to amend the Federal Trade Commission's ("FTC's") Safeguards Rule. This survey also summarizes recent cases on whether an entity is a consumer reporting agency ("CRA"), determining when plaintiffs have Article III standing to maintain Fair Credit Reporting Act ("FCRA")[3] claims, and CRAs' obligations to reinvestigate dispute letters sent by credit repair organizations.

Financial Privacy Enforcement Actions

Data Breach Settlement with Equifax

In July 2019, the CFPB, the FTC, forty-eight states, the District of Columbia, and Puerto Rico announced a settlement with Equifax Inc. regarding its 2017 data breach.[4] The CFPB alleged that Equifax engaged in unfair acts and practices by failing to provide reasonable security for sensitive consumer personal

* Andrew Soukup is a partner in the Washington, D.C. office of Covington & Burling LLP who specializes in financial services litigation. David A. Stein is of counsel in the Washington, D.C. office of Covington & Burling LLP who specializes in providing regulatory advice on credit reporting, privacy, consumer financial services, and fintech. Lucille C. Bartholomew is an associate in the Washington, D.C. office of Covington & Burling LLP.

1. *See* Andrew Soukup, David A. Stein & Lucille C. Bartholomew, *Fair Credit Reporting Act and Financial Privacy Update—2018*, 74 Bus. Law. 495 (2019) (in the 2019 *Annual Survey*).

2. *See, e.g.*, Andrew M. Smith, Andrew Soukup & Lucille C. Bartholomew, *Fair Credit Reporting Act and Financial Privacy Update—2017*, 73 Bus. Law. 441 (2018) (in the 2018 *Annual Survey*).

3. Pub. L. No. 91-508, tit. VI, 84 Stat. 1114, 1127–36 (1970) (codified as amended at 15 U.S.C. §§ 1681–1681x (2018)).

4. *See* Press Release, Consumer Fin. Prot. Bureau, CFPB, FTC and States Announce Settlement with Equifax Over 2017 Data Breach (July 22, 2019), https://www.consumerfinance.gov/about-us/newsroom/cfpb-ftc-states-announce-settlement-with-equifax-over-2017-data-breach/; Press Release, Fed. Trade Comm'n, Equifax to Pay $575 Million as Part of Settlement with FTC, CFPB, and States Related to 2017 Data Breach (July 22, 2019), https://www.ftc.gov/news-events/press-releases/2019/07/equifax-pay-575-million-part-settlement-ftc-cfpb-states-related.

information,[5] and by misrepresenting that it limited access to consumer personal information to certain employees and had reasonable safeguards in place to protect personal information.[6] The CFPB also alleged that Equifax's response to the data breach involved unfair acts or practices because the incident response website and the security freeze personal identification numbers used to access the site were vulnerable to hackers and exposed consumers to additional risk of harm.[7] The FTC separately made similar allegations and also alleged that Equifax violated the Gramm-Leach-Bliley Act ("GLBA") Safeguards Rule.[8]

Under a global settlement, Equifax will pay up to $700 million in civil money penalties and customer restitution, including a $100 million civil money penalty imposed by the CFPB,[9] up to $425 million in customer restitution imposed by the FTC,[10] and additional penalties and customer restitution required by state attorneys general.[11]

FTC Privacy Settlement with Facebook

In July 2019, the FTC announced a settlement with Facebook, Inc. regarding allegations that it failed to protect consumers' privacy as required by a 2012 FTC consent order.[12] Among other things, the FTC alleged that Facebook engaged in a deceptive act or practice when the company shared the data of Facebook "friends" with third-party applications, even when the "friends" had more

5. *See* Complaint for Permanent Injunction and Other Relief at 20–21, CFPB v. Equifax, Inc., No. 1:19-cv-03300-TWT (N.D. Ga. July 22, 2019), https://files.consumerfinance.gov/f/documents/cfpb_equifax-inc_complaint_2019-07.pdf.

6. *Id.* at 21–22.

7. *Id.* at 22–23.

8. *See* Complaint for Permanent Injunction and Other Relief at 1, FTC v. Equifax Inc., No. 1:19-mi-99999-UNA (N.D. Ga. July 22, 2019), https://www.ftc.gov/system/files/documents/cases/172_3203_equifax_complaint_7-22-19.pdf.

9. *See* Stipulated Order for Permanent Injunction and Monetary Judgment at 49–50, 59–60, CFPB v. Equifax, Inc., No. 1:19-cv-03300-TWT (N.D. Ga. July 23, 2019), https://files.consumerfinance.gov/f/documents/cfpb_equifax-inc_proposed-stipulated-order_2019-07.pdf.

10. *See* Stipulated Order for Permanent Injunction and Monetary Judgment at 27–49, FTC v. Equifax Inc., No. 1:19-mi-99999-UNA (N.D. Ga. July 22, 2019), https://www.ftc.gov/system/files/documents/cases/172_3203_equifax_proposed_order_7-22-19.pdf.

11. *See, e.g.*, Press Release, N.Y. Attorney Gen., Attorney General James Holds Equifax Accountable by Securing $600 Million Payment in Largest Data Breach Settlement in History (July 22, 2019), https://ag.ny.gov/press-release/attorney-general-james-holds-equifax-accountable-securing-600-million-payment-largest; Press Release, Cal. Attorney Gen., Attorney General Becerra Announces Settlement Against Equifax Providing $600 Million in Consumer Restitution and State Penalties (July 22, 2019), https://oag.ca.gov/news/press-releases/attorney-general-becerra-announces-settlement-against-equifax-providing-600.

12. Press Release, Fed. Trade Comm'n, FTC Imposes $5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook (July 24, 2019), https://www.ftc.gov/news-events/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions; *see* Complaint for Civil Penalties, Injunction, and Other Relief at 1, United States v. Facebook, Inc., No. 1:19-cv-02184 (D.D.C. July 24, 2019), https://www.ftc.gov/system/files/documents/cases/182_3109_facebook_complaint_filed_7-24-19.pdf [hereinafter Facebook Complaint]; *see also In re* Facebook, Inc., No. C-4365 (F.T.C. July 27, 2012) (decision and order), https://www.ftc.gov/sites/default/files/documents/cases/2012/08/120810facebookdo.pdf.

restrictive privacy settings.[13] The FTC also alleged that Facebook acted deceptively when it disclosed to users that it would collect phone numbers for a security feature, but failed to disclose that Facebook would use the phone numbers for marketing.[14] The complaint also alleged that, through its privacy policy, Facebook deceptively implied that users would need to opt in to facial recognition technology when an older version of this technology was turned on by default and consumers had to opt out.[15]

Based on these allegations, the FTC assessed an unprecedented $5 billion penalty against Facebook.[16] In addition, the settlement requires Facebook to make a number of changes to its privacy practices and imposes various compliance requirements on Facebook, including establishing an independent privacy committee of the board of directors vested with specific authority, additional layers of approval and other governance matters, and implementing a comprehensive privacy program with enhanced oversight of third parties.[17] Two of the five FTC commissioners dissented from the settlement based in large part on the immunity granted to Facebook and its senior executives.[18]

Privacy Notice Enforcement Actions

The FTC and CFPB each brought enforcement actions addressing lenders' failures to provide consumers with GLBA privacy notices. In October 2018, the FTC filed an amended complaint against LendingClub Corporation in the U.S. District Court for the Northern District of California that alleged violations of the GLBA's Privacy Rule in addition to other alleged violations of law.[19] The FTC alleged that Lending Club failed to deliver its initial privacy notice in a way that consumers could reasonably be expected to receive it because, instead of requiring consumers to acknowledge receipt of the notice, LendingClub required them to agree to its terms of use, which included a link to another lengthy document that had a link to the privacy policy.[20] Consumers were only provided a link leading directly to the privacy notice after they applied for the loan.[21] The FTC alleged that this failed to provide a clear and conspicuous privacy

13. *See* Facebook Complaint, *supra* note 12, at 12–20, 43–45.
14. *See id.* at 36–39, 47–48.
15. *See id.* at 39–42, 47.
16. *See* Stipulated Order for Civil Penalty, Monetary Judgment, and Injunctive Relief at 3, United States v. Facebook, Inc., No. 1:19-cv-02184 (D.D.C. July 24, 2019), https://www.ftc.gov/system/files/documents/cases/182_3109_facebook_order_filed_7-24-19.pdf.
17. *See id.* at 4.
18. *See* Dissenting Statement of Commissioner Rebecca Kelly Slaughter: *In re* Facebook, Inc. 2 (July 24, 2019), https://www.ftc.gov/system/files/documents/public_statements/1536918/182_3109_slaughter_statement_on_facebook_7-24-19.pdf; Dissenting Statement of Commissioner Rohit Chopra: *In re* Facebook, Inc. 19–20 (July 24, 2019), https://www.ftc.gov/system/files/documents/public_statements/1536911/chopra_dissenting_statement_on_facebook_7-24-19.pdf.
19. *See* First Amended Complaint at 27–28, FTC v. LendingClub Corp., No. 3:18-cv-020454-JSC (N.D. Cal. Oct. 22, 2018), https://www.ftc.gov/system/files/documents/cases/lendingclub_corporation_first_amended_complaint.pdf.
20. *Id.* at 25.
21. *Id.* at 25–26.

notice to consumers before they submitted nonpublic personal information to LendingClub.[22]

Credit Reporting Enforcement Actions

The CFPB brought three enforcement actions during the past year based on credit reporting issues. In December 2018, the CFPB entered into a consent order with State Farm Bank, FSB ("State Farm") for allegedly improperly obtaining consumer credit reports and furnishing inaccurate or incomplete information to CRAs in violation of the FCRA.[23] State Farm agents allegedly generated credit inquiries for consumers who did not wish to apply for credit by inputting the wrong consumer information into credit applications and by initiating "applications for consumers for the purpose of soliciting those consumers."[24] The CFPB also alleged that State Farm furnished inaccurate consumer information to CRAs that contradicted other consumer data that State Farm had.[25] The consent order required State Farm to implement policies and procedures to address the CFPB's allegations, but did not require State Farm to pay a civil monetary penalty or provide any customer restitution.[26]

In October 2018, the CFPB entered into a consent order with online retailer Bluestem Brands, Inc. ("Bluestem") over allegations that it failed to timely forward its customers' payments to third-party debt buyers.[27] The CFPB alleged that, as a result, Bluestem engaged in an unfair act or practice by subjecting consumers to inaccurate credit reporting by debt buyers and misleading debt-collection efforts.[28] The consent order required Bluestem to pay a $200,000 civil monetary penalty and implement policies and procedures to ensure that consumers receive notice when Bluestem sells their debt, and that Bluestem timely forward payments to appropriate debt buyers.[29]

Also in October 2018, the CFPB entered into a consent order with Cash Express, LLC ("Cash Express") over allegations that it falsely represented to consumers that it might furnish their information to CRAs, among other things.[30] The CFPB alleged that Cash Express engaged in a deceptive act or practice by representing in its loan applications, collection letters, privacy policy disclosures, and loan agreements that it "may" report information to CRAs, when it did not furnish

22. *Id.* at 26, 28.

23. *See* Consent Order at 1–2, *In re* State Farm Bank, FSB, CFPB No. 2018-BCFP-0009 (Dec. 5, 2018), https://files.consumerfinance.gov/f/documents/bcfp_state-farm-bank_consent-order.pdf.

24. *Id.* at 6–7.

25. *Id.* at 8.

26. *Id.* at 12–24.

27. *See* Consent Order at 2, *In re* Bluestem Brands, Inc., CFPB No. 2018-BCFP-0006 (Oct. 2, 2018), https://files.consumerfinance.gov/f/documents/bcfp_bluestem-brands-inc_consent-order_2018-10.pdf.

28. *See id.* at 2, 4–5 (discussing debt-collection-related injuries).

29. *Id.* at 7–11.

30. Consent Order at 6–8, *In re* Cash Express, LLC, CFPB No. 2018-BCFP-0007 (Oct. 23, 2018), https://files.consumerfinance.gov/f/documents/bcfp_cash-express-llc_consent-order_2018-10.pdf.

information to CRAs during the relevant period.[31] According to the CFPB, these representations were likely to mislead consumers and may have caused consumers to pay debts to Cash Express to avoid negative credit reporting.[32] The consent order prohibits Cash Express from suggesting that it might furnish information to CRAs unless it "regularly furnish[es]" such information,[33] and orders Cash Express to pay a civil money penalty of $200,000 for the alleged violations.[34]

FTC Safeguards Rule Proposal

On March 5, 2019, the FTC released a proposal to amend the existing Standards for Safeguarding Customer Information ("Safeguards Rule"), which the FTC issued in 2002 pursuant to the GLBA.[35] The FTC's existing Safeguards Rule applies to financial institutions that are not subject to similar information security requirements adopted by other federal financial regulators.[36] The existing Safeguards Rule applies to businesses "significantly" engaged in providing financial products or services, as defined in section 4(k) of the Bank Holding Company Act,[37] but it does not apply to businesses engaged in "occasional" financial activities.[38]

The proposed amendments would "retain the process-based approach of the [existing] Rule, while providing a more detailed map of what information security plans must address."[39] Although the FTC recognized that "the flexibility of the current Safeguards Rule is a strength that allows the Rule to adapt to changing technology and threats," it believes that "more specific requirements will benefit financial institutions by providing them with more guidance and certainty in developing their information security programs."[40] The proposed amendments would expand the scope of the Safeguards Rule to apply to financial institutions engaged in "incidental" activities, including finders, and align the scope of activities covered by the FTC's Safeguards Rule with those covered by the federal banking agencies' information security standards.[41]

The proposed amendments would augment the current Safeguards Rule in several respects. It would require financial institutions to designate a qualified

31. *Id.* at 7–8.
32. *Id.* at 8.
33. *Id.* at 11.
34. *Id.* at 16.
35. Standards for Safeguarding Customer Information, 84 Fed. Reg. 13158, 13160 (proposed Apr. 4, 2019) (to be codified at 16 C.F.R. pt. 314) [hereinafter Proposed Safeguards Rule]; *see* Pub. L. No. 106-102, tit. V, 113 Stat. 1338, 1436–50 (1999) (codified as amended at 15 U.S.C. §§ 6801–6809, 6821–6827 (2018)).
36. *See* 16 C.F.R. pt. 314 (2019).
37. *Id.* § 313.3(k); *see* 12 U.S.C. § 1843(k) (2018).
38. 16 C.F.R. § 313.3(k)(4) (2019).
39. Proposed Safeguards Rule, *supra* note 35, at 13160.
40. *Id.*
41. *Id.* at 13174 (to be codified at 16 C.F.R. § 314.2(f)(1) ("An institution that is . . . significantly engaged in activities incidental to . . . financial activities is a financial institution.")). The expanded definition would also apply to the FTC's Privacy Rule. *Id.* at 13164; *see* 16 C.F.R. pt. 313 (2019).

individual as chief information security officer ("CISO") to oversee, implement, and enforce the information security program in place of the current requirement to designate an employee or employees to "coordinate" the information security program.[42] The CISO would be required to report at least annually to the board of directors about issues related to the information security program.[43]

The proposed amendments would also add to the existing Safeguards Rule's requirement to identify and assess "reasonably foreseeable risks" by requiring financial institutions to develop written risk assessments that include specific components.[44] For example, financial institutions would be required to include in the written risk assessment the criteria for evaluating security risks, confidentiality, and the adequacy and effectiveness of existing controls, among other things.[45] Financial institutions would also be required to include a description of how any risks identified as a result of the risk assessment will be mitigated and/or how the information security program addresses any such risks.[46]

The proposed amendments would add ten new specific safeguards that must be included in a financial institution's information security program.[47] Among these would be implementation of access control measures to information security systems to protect against unauthorized access to customer information;[48] requiring multi-factor authentication for individuals accessing customer information;[49] restricting access to physical locations that contain customer information;[50] encrypting customer information at rest and in transit;[51] and adopting "secure development practices" for applications developed in-house for transmitting, storing, or accessing customer information, and procedures for testing, assessing, or evaluating the security of applications developed externally for the same purposes.[52]

42. Proposed Safeguards Rule, *supra* note 35, at 13175 (to be codified at 16 C.F.R. § 314.4(a) ("In order to develop, implement, and maintain your information security program, you shall . . . [d]esignate a qualified individual responsible for overseeing and implementing your information security program and enforcing your information security program (for purposes of this part, 'Chief Information Security Officer' or 'CISO').")); *see* 16 C.F.R. § 314.4(a) (2019) ("In order to develop, implement, and maintain your information security program, you shall . . . [d]esignate an employee or employees to coordinate your information security program.").

43. Proposed Safeguards Rule, *supra* note 35, at 13176 (to be codified at 16 C.F.R. § 314.4(i)).

44. *See id*. at 13175 (to be codified at 16 C.F.R. § 314.4(b)).

45. *See id.* (to be codified at 16 C.F.R. § 314.4(b)(1)).

46. *See id.* at 13175–76 (to be codified at 16 C.F.R. § 314.4(b), (g)).

47. *See id*. (to be codified at 16 C.F.R. § 314.4(c)(1)–(10)).

48. *See id*. at 13175 (to be codified at 16 C.F.R. § 314.4(c)(1)).

49. *See id.* (to be codified at 16 C.F.R. § 314.4(c)(6)). The proposed amendment includes an exception if the CISO has approved, in writing, the use of a "reasonably equivalent" or more secure access control. *Id*.

50. *See id.* (to be codified at 16 C.F.R. § 314.4(c)(3)).

51. *Id*. (to be codified at 16 C.F.R. § 314.4(c)(4)). The proposed amendment includes a limited exception: "To the extent [the financial institution] determine[s] that encryption of customer information, either in transit over external networks or at rest, is infeasible, [the financial institution] may instead secure such customer information using effective alternative compensating controls reviewed and approved by your CISO." *Id*.

52. *Id.* (to be codified at 16 C.F.R. § 314.4(c)(5)).

The proposed amendments would also require regular testing and monitoring of controls used to "detect actual and attempted attacks on, or intrusions into, the information systems."[53] In addition, financial institutions would be required to perform effective continuous monitoring or annual penetration testing and biannual vulnerability assessments.[54] Financial institutions would have to enhance security training for their personnel and periodically assess their service providers based on the risk that each service provider presents and the adequacy of service providers' safeguards.[55] Finally, financial institutions would have to prepare detailed written incident response plans.[56]

Recognizing the potential adverse impacts of more detailed and prescriptive requirements on smaller companies, the FTC proposed a limited exception for financial institutions that maintain customer information on fewer than 5,000 consumers.[57] This exception would allow qualified institutions not to have to comply with the new, specific requirements for developing a written risk assessment.[58] They would also not be required to perform continuous monitoring or periodic penetration testing and vulnerability assessments, establish a written incident response plan, or require the CISO to report to the board.[59]

Litigation Developments

Determining What Constitutes a "Consumer Reporting Agency"

A pair of recent decisions sheds light on the circumstances under which companies are considered "consumer reporting agencies" for purposes of the FCRA. As discussed in the previous *Survey*,[60] the district court, in *Kidd v. Thomson Reuters Corp.*,[61] adopted a "totality of the circumstances" test and held that Thomson Reuters was not a CRA because it did not assemble or evaluate information "for the purpose of furnishing consumer reports to third parties" in its subscription-based online research platform ("CLEAR").[62] The Second Circuit affirmed the district court's use of its "totality" test, holding that Thomson Reuters did not intend to furnish consumer reports through its CLEAR platform and therefore that it did not violate the FCRA.[63] The Second Circuit found that Thomson Reuters' "numerous—and effective—measures" to prevent CLEAR reports from being used as consumer reports demonstrated its lack of intent to provide such reports.[64] The measures included contractual restrictions on use of the reports;

53. *Id.* at 13176 (to be codified at 16 C.F.R. § 314.4(d)(1)).
54. *See id.* (to be codified at 16 C.F.R. § 314.4(d)(2)).
55. *See id.* (to be codified at 16 C.F.R. § 314.4(e)–(f)).
56. *See id.* (to be codified at 16 C.F.R. § 314.4(h)).
57. *See id.* (to be codified at 16 C.F.R. § 314.6).
58. *See id.* at 13175–76.
59. *See id.*
60. *See* Soukup, Stein & Bartholomew, *supra* note 1, at 504–05.
61. 299 F. Supp. 3d 400 (S.D.N.Y. 2017), *aff'd*, 925 F.3d 99 (2d Cir. 2019).
62. *Id.* at 403–05 (quoting 15 U.S.C. § 1681a(f)).
63. *See Kidd*, 925 F.3d at 107, 109.
64. *Id.* at 107.

marketing materials consistent with the contractual restrictions; due diligence on potential subscribers for their intended use of CLEAR; periodic recertification requirements prohibiting the use of CLEAR for FCRA purposes; investigation of potential misuses; and taking appropriate remedial actions for confirmed misuses of CLEAR reports.[65] Thus, Thomson Reuters did not qualify as a CRA "even in the few instances where CLEAR was misused for FCRA purposes."[66]

In *Zabriskie v. Federal National Mortgage Association*,[67] the Ninth Circuit held that Fannie Mae was not a CRA based on its Desktop Underwriter ("DU") tool, which Fannie Mae licenses to mortgage lenders for the purpose of determining whether it will purchase mortgages from them.[68] The plaintiffs were unable to obtain a mortgage because the DU tool incorrectly indicated a foreclosure. They claimed that Fannie Mae was a CRA and did not follow "reasonable procedures to assure maximum possible accuracy."[69] The Ninth Circuit reversed the district court's holding that Fannie Mae is a CRA when it licenses the DU tool to lenders.[70] It found that Fannie Mae is not a CRA because it does not regularly engage in assembling or evaluating consumer information and it does not assemble or evaluate consumer information "for the purpose of furnishing consumer reports to third parties."[71] Rather, the *Zabriskie* court found that Fannie Mae merely provides software that allows lenders to assemble or evaluate such information and provides the DU tool for no purpose other than to determine a loan's eligibility for subsequent purchase by Fannie Mae.[72]

Reinvestigation Obligations for Dispute Letters

The Ninth Circuit ruled, in *Warner v. Experian Information Solutions, Inc.*[73] that CRAs have no obligation under the FCRA to respond to letters sent by a credit repair organization on a consumer's behalf when the consumer "played almost no part in submitting the dispute letter."[74] Credit repair organization Go Clean Credit wrote to Experian on behalf of a consumer asserting that several items in the consumer's credit file were incorrect and asking Experian to investigate the items' accuracy. However, the FCRA only requires CRAs to investigate disputed items in a consumer's credit file if the consumer "directly" notifies the agency of the dispute.[75] Because the consumer "played no part in drafting, finalizing, or sending the letters Go Clean Credit sent to Experian on his behalf," the

65. *Id.* at 107–08.
66. *Id.* at 108.
67. 912 F.3d 1192 (9th Cir. 2019).
68. *Id.* at 1195.
69. *Id.* at 1196 (quoting 15 U.S.C. § 1681e(b)).
70. *Id.* at 1196–97.
71. *Id.* (quoting 15 U.S.C. § 1681a(f)).
72. *Id.* at 1197 ("[W]hen a person uses a tool to perform an act, the person is engaged in the act; the tool's maker is not.").
73. 931 F.3d 917 (9th Cir. 2019).
74. *Id.* at 921.
75. 15 U.S.C. § 1681i (2018).

Ninth Circuit held that those letters "did not come directly from him," and Experian had no obligation to conduct a reinvestigation.[76]

Further Applications of *Spokeo*

During the past year, federal courts continued to reach different conclusions regarding whether consumers demonstrated an injury-in-fact sufficient to satisfy Article III's standing requirements for FCRA claims under *Spokeo, Inc. v. Robins*.[77] For example, two courts found that Article III standing existed when a consumer was deprived a copy of her background report.[78] On the other hand, courts found that Article III standing did not exist to: assert claims alleging procedural violations related to access to a background report when the consumer consented to access the report;[79] challenge a failure to notify job applicants of their FCRA rights;[80] sue a former employer over a failure to provide a summary of an investigation that led to firing employees when they could not identify an employer that refused to hire them as a result of such information;[81] and challenge a check verification company's omission of certain information from a copy of the company's file provided to a consumer.[82]

Earlier *Surveys* discussed lawsuits that challenged how information was reported about consumers' bankruptcies, which courts dismissed on accuracy grounds.[83] In *Jaras v. Equifax, Inc.*,[84] the Ninth Circuit resolved some of these lawsuits on an alternative ground, by holding that consumers lacked standing to assert such challenges. The plaintiffs claimed that the manner in which several CRAs and their lenders provided information about their accounts was inconsistent with the treatment of those accounts under their confirmed Chapter 13 plans.[85] The Ninth Circuit held that the plaintiffs lacked standing to assert those challenges because they failed to allege "that they tried to enter any financial transaction for which their credit reports or scores were viewed at all, or that they plan to imminently do so, let alone that the alleged inaccuracies in their credit reports would make a difference to such a transaction."[86]

Federal appellate courts continued to divide over the circumstances under which a card number truncation receipt violation is sufficient to establish a

76. *Warner*, 931 F.3d at 919.
77. 136 S. Ct. 1540 (2016). In *Spokeo,* the U.S. Supreme Court held that "Article III standing requires a concrete injury even in the context of a statutory violation." *Id.* at 1549.
78. Long v. Se. Pa. Transp. Auth., 903 F.3d 312, 324–25 (3d Cir. 2018); Robertson v. Allied Sols., LLC, 902 F.3d 690, 699 (7th Cir. 2018).
79. Auer v. Trans Union, LLC, 902 F.3d 873, 878–79 (8th Cir. 2018).
80. *Long*, 903 F.3d at 325.
81. Rivera v. Allstate Ins. Co., 913 F.3d 603, 617–18 (7th Cir. 2018).
82. Huff v. TeleCheck Servs., Inc., 923 F.3d 458, 468–69 (6th Cir. 2019).
83. *See* Soukup, Stein & Bartholomew, *supra* note 1, at 505–06; Smith, Soukup & Bartholomew, *supra* note 2, at 448–49.
84. 766 F. App'x 492 (9th Cir. 2019).
85. *Id.* at 493–94.
86. *Id.* at 494.

"real," concrete injury for an FCRA claim as *Spokeo* requires.[87] In *Jeffries v. Volume Services America, Inc.*,[88] the plaintiff received a receipt from the defendant showing all sixteen digits of her credit card number and expiration date in violation of the FCRA, which prohibits printing "more than the last 5 digits of the card number or the expiration date" on a receipt.[89] The D.C. Circuit held that a "violation as egregious as the one committed by" the defendant was a "concrete injury in fact" because the plaintiff was unable to use her card "without incurring an increased risk of identity theft."[90] The D.C. Circuit's ruling is consistent with an Eleventh Circuit case that concluded that showing ten digits on a receipt constituted a "concrete injury" sufficient for Article III standing.[91] These cases conflict with decisions from a number of other appellate courts,[92] including most recently the Third Circuit's decision in *Kamal v. J. Crew Group, Inc.*,[93] which held that the plaintiff lacked standing when he received a receipt showing the first six and last four digits of his credit card number.[94]

87. Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1549 (2016); *see* 15 U.S.C. § 1681c(g)(1) (2018).
88. 928 F.3d 1059 (D.C. Cir. 2019).
89. *Id.* at 1062 (quoting 15 U.S.C. § 1681c(g)(1)).
90. *Id.* at 1066.
91. Muransky v. Godiva Chocolatier, Inc., 922 F.3d 1175, 1192 (11th Cir. 2019).
92. *See, e.g.*, Basset v. ABM Parking Servs., Inc., 883 F.3d 776, 783 (9th Cir. 2018); Katz v. Donna Karan Co., 872 F.3d 114, 121 (2d Cir. 2017); Meyers v. Nicolet Rest. of De Pere, LLC, 843 F.3d 724, 729 (7th Cir. 2016).
93. 918 F.3d 102 (3d Cir. 2019).
94. *Id.* at 106, 119–20.