

# Stanford **Technology** Law Review

## The 10 Year Anniversary of the FTC's Data Security Program: Has the Commission Finally Gotten Too Big for Its Breaches?

DAVID ALAN ZETOONY\*

CITE AS: 2011 STAN. TECH. L. REV. 12

<http://stlr.stanford.edu/pdf/zetoony-ten-year-anniversary.pdf>

### ABSTRACT

¶1 The Federal Trade Commission is the primary federal agency responsible for enforcing the data security laws on private sector entities. Since 2002, the FTC has brought a series of enforcement actions against companies that have concluded in consent decrees stating that those companies violated the law by having insufficient data security practices. The FTC recently brought three new actions that purport to hold companies responsible for the substandard security practices of their business customers. While the FTC has suggested that a duty to police business customers' data security practices applies broadly to all companies that hold sensitive personal information, the FTC has failed to adequately explain the legal basis of such a duty.

### INTRODUCTION

¶2 An online company provides products to individuals and small businesses. Like most online companies, it collects various types of information from its customers such as email addresses for notifications, mailing addresses for product shipment, and credit and debit card numbers for payment.

¶3 From its inception, the company's management takes data security very seriously. The company forms an interdepartmental team to assess potential vulnerabilities to the company's website, computers, and physical building, creates a written data security plan and policy, and, each year, conducts a data inventory to help identify where it stores the information that it collects and who has access to that information. As the company grows, it may even hire a Chief Privacy Officer who does everything from training employees on how to shred old invoices to making sure that the company's growing list of outside vendors don't have disparate data security practices. This company has complied with its obligation to secure consumer data, right?

---

\* © 2011, David Alan Zetoony. David Zetoony is a partner at Bryan Cave LLP in Washington, D.C. and the leader of the firm's data privacy and security practice. He has represented companies before the FTC in matters involving advertising, data privacy, and data security. The author wishes to thank Dana Rosenfeld for providing her thoughts and comments on an early draft of this article

¶4 Maybe not. The Federal Trade Commission's settlements with SettlementOne Credit, ACRAnet, Inc., and Fajilan and Associates, Inc. suggest that in addition to enacting good practices for their own operations and making sure that their vendors do the same, companies are responsible for making sure that their *customers* have adequate data security. Although the FTC cites several statutes as the basis for this "duty to police customers," it is not at all clear that the FTC's theory could survive judicial scrutiny. Part I of this article provides a brief history of the FTC's success over the past ten years to position itself as the primary federal regulator concerning issues of data security. Part II discusses the FTC's recent enforcement actions and settlements with SettlementOne Credit, ACRAnet, and Fajilan. Part III analyzes the limits of the FTC's data security enforcement powers. As part of this analysis, it reviews the scope of the new duty that the Commission proposes as part of the Reseller settlements, and analyzes whether the duty that the Commission seeks to impose can be supported by the Commission's authorizing legislation. Finally the article concludes that the Commission's attempt to create a new duty to police customers lacks firm statutory support and may not be successful if challenged in court.

### I. A BRIEF HISTORY OF THE FTC'S DATA PRIVACY AND SECURITY PROGRAM

¶5 The legal theory that companies have a duty to safeguard consumer sensitive information that is within their possession is relatively new. Congress first imposed this obligation in the late 1990s to members of specific industries that were perceived to possess particularly sensitive information, such as health care providers pursuant to the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), and financial institutions pursuant to the Gramm-Leach-Bliley Act of 1999 ("GLBA").<sup>1</sup>

¶6 Outside of these select industries, Congress did not appoint a single federal agency to enforce data privacy and security standards. Nonetheless, beginning in 2002 with its enforcement action against *Petco*, the FTC began using its deception authority to pursue companies that misrepresented the level or degree of security that they applied to consumer data.<sup>2</sup> A few years later, the Commission used its unfairness authority to pursue a claim that a company had used inadequate security to protect consumer information even when the company made no representations concerning the level or degree of security that it applied to consumer data.<sup>3</sup>

¶7 Since 2002, the contours of companies' duty to safeguard personal information—and the repercussions for failing to meet that duty—have "become a central focus" of the FTC.<sup>4</sup> As the Commission's Director of the Bureau of Consumer Protection recently testified before Congress:

As the nation's consumer protection agency, the FTC is committed to protecting consumer privacy and promoting data security in the private sector and has brought more than 30 law enforcement actions against businesses that allegedly failed to protect consumers' personal information appropriately . . . . Data security is of critical importance to consumers. If companies do not protect the personal information they collect and store, that information could fall into the wrong hands, resulting in fraud and other harm, and consumers could lose confidence in the marketplace. Accordingly, the Commission has undertaken substantial efforts to promote data security in the private sector through law enforcement, education, and policy initiatives.<sup>5</sup>

<sup>1</sup> Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936, (1996). Gramm-Leach-Bliley Act, Pub. L. No. 106-102, 113 Stat. 1338, (1999).

<sup>2</sup> The *Petco* complaint can be found at: <http://www.ftc.gov/os/caselist/0323221/041108comp0323221.pdf>. The FTC's deception authority refers to the Commission's ability to pursue "deceptive acts or practices in or affecting commerce." 15 U.S.C. § 45(a)(1) (2011).

<sup>3</sup> See Complaint, In the Matter of BJ's Wholesale Club, Inc., FTC Case No. C-4148, *available at* <http://www.ftc.gov/os/caselist/0423160/092305comp0423160.pdf>. The FTC's unfairness authority refers to the Commission's ability to pursue "unfair methods of competition" and "unfair . . . acts or practices in or affecting commerce." 15 U.S.C. § 45(a)(1) (2011).

<sup>4</sup> FED. TRADE COMM'N, FISCAL YEAR 2012 CONGRESSIONAL BUDGET JUSTIFICATION SUMMARY 1, 6 (2011), *available at* <http://www.ftc.gov/ftc/oed/fmo/budgetsummary12.pdf>.

<sup>5</sup> *Hearing on Data Security Before the H. Subcomm. on Commerce, Mfg., and Trade of the H. Comm. on Energy and Commerce*, 112th Cong., 1 (2011) (statement of David C. Vladeck, Dir. of the Bureau of Consumer Prot. at the Fed. Trade Comm'n), *available at*

¶8 Although it is true that the Commission has brought more than 30 data privacy and security enforcement actions, the Commission has yet to litigate a single case.<sup>6</sup> Instead, the Commission has entered into a string of consent orders with the companies that it has investigated, most, if not all, negotiated before a complaint was filed. In the absence of case law, the legal community has used these consent orders as evidence of the types of practices that the Commission believes violate the law, and as a benchmark for the type of relief that would be available to the Commission if it were to proceed to trial against a company that is alleged to have provided inadequate security.<sup>7</sup> In essence, the Commission's ten year streak of consent orders has de facto guided the development of what are commonly referred to as the data security laws.

## II. THE FTC'S COMPLAINTS AGAINST SETTLEMENTONE CREDIT, ACRANET, AND FAJILIAN

¶9 Three of the most recent FTC data security consent orders involved allegations against SettlementOne Credit, ACRANet, and Fajilan (the "Resellers"). The Resellers aggregate credit reports from the national credit reporting agencies (i.e., Equifax, Experian, and TransUnion) in order to sell merged reports to businesses such as mortgage brokers who use the reports to determine consumers' eligibility for credit. Over a period of several years, hackers allegedly gained access to the merged credit reports. They did not do so by breaching the Resellers' computer systems. Rather, they hacked into the computers of the Resellers' customers—the businesses and mortgage brokers that had ordered the consumer reports.<sup>8</sup> After the hackers entered the customers' networks they were able to collectively access 1,800 consumer reports.<sup>9</sup> Although the FTC has not provided details concerning how the hackers gained access to the computer systems, or whether the attacks were coordinated, the Commission stated that if the business customers had "basic security measures in place, such as firewalls and updated antivirus software," the breaches could have been prevented.<sup>10</sup>

¶10 The FTC did not proceed against the hackers for causing the breaches, nor did the FTC proceed against the businesses that had failed to install firewalls and antivirus software to prevent the breaches. Instead, on February 3, 2011, the FTC released complaints against, and proposed settlement agreements with, the Resellers. The complaints alleged that the Resellers should have taken steps to prevent the breaches by "evaluating the security of end user's computer networks," "requiring [end users to implement] appropriate information security measures," and "training end user clients" concerning data security practices.<sup>11</sup> The Commission suggests, for instance, that the Resellers should have required that "new and existing end user clients submit . . . documentation demonstrating that the clients' computer systems were virus free and otherwise properly protected."<sup>12</sup> According to the FTC, the Resellers' failure to police their business customers for good

<http://www.ftc.gov/opa/2011/05/pdf/110504datasecurityhouse.pdf>.

<sup>6</sup> A list of the Commission's data security cases can be found in the prepared statement of the Federal Trade Commission to the House of Representatives Subcommittee on Commerce, Manufacturing and Trade. *See id.* at 3 n.6.

<sup>7</sup> Indeed, the First Circuit has referred to the "substantial body of FTC complaints and consent decrees" that address "unfair" data security practices as "instructive." *In re: TJX Cos. Retail Security Breach Litig.*, 564 F.3d 489, 496 (1st Cir. 2009).

<sup>8</sup> The complaints against SettlementOne and ACRANet indicate that the hackers gained access to SettlementOne end user clients, and ACRANet end user clients. Complaint ¶ 10, SettlementOne Credit Corp., File No. 082-3208 (FTC Feb. 3, 2011), *available at* <http://www.ftc.gov/os/caselist/0823208/110203settlemtonemcpt.pdf> [hereinafter SettlementOne Complaint]; Complaint ¶ 9, ACRANet, Inc., File No. 092-3088 (FTC Feb. 3, 2011), *available at* <http://www.ftc.gov/os/caselist/0923088/110203acranetmpt.pdf> [hereinafter ACRANet Complaint]. The complaint against Fajilan suggests that the hackers gained access to both Fajilan's network and the networks of Fajilan's "end user clients." Complaint ¶ 10, Fajilan and Assocs., File No. 092-3089 (FTC Feb. 3, 2011), *available at* <http://www.ftc.gov/os/caselist/0923089/110203statewidemcpt.pdf> [hereinafter Fajilan Complaint].

<sup>9</sup> The FTC alleges that hackers accessed 784 consumer reports from the networks of SettlementOne's clients, 694 consumer reports from the networks of ACRANet's clients, and 323 consumer reports from Fajilan's clients. SettlementOne Complaint, *supra* note 8 ¶ 10; ACRANet Complaint, *supra* note 8 ¶ 9; Fajilan Complaint, *supra* note 8, ¶ 10.

<sup>10</sup> SettlementOne Complaint, *supra* note 8, ¶ 9; ACRANet Complaint, *supra* note 8, ¶ 8; Fajilan Complaint, *supra* note 8, ¶ 9.

<sup>11</sup> SettlementOne Complaint, *supra* note 8, ¶ 8(c); ACRANet Complaint, *supra* note 8, ¶ 7(c); Fajilan Complaint, *supra* note 8, ¶ 8(c).

<sup>12</sup> ACRANet Complaint, *supra* note 8, ¶ 10; *see* SettlementOne Complaint, *supra* note 8, ¶ 11; Fajilan Complaint, *supra* note 8, ¶ 11. It is not clear whether the FTC suggests that the Resellers should have required such documentation before the breaches

data security practices violated the GLBA, the Fair Credit Reporting Act (“FCRA”), and constituted an “unfair practice” under the FTC Act.<sup>13</sup> A statement issued by four of the Commissioners—Brill, Leibowitz, Rosch, and Ramirez—further stated:

[W]e are also cognizant of the fact that these are the first cases in which the Commission has held resellers responsible for downstream data protection failures. Looking forward, the actions we announce today should put resellers – *indeed, all of those in the chain of handling consumer data* – on notice of the seriousness with which we view their legal obligations to proactively protect consumers’ data. The Commission should use all of the tools at its disposal to protect consumers from the enormous risks posed by security breaches that may lead to identity theft.<sup>14</sup>

¶11 On August 17, 2011, the FTC approved the settlements and entered formal orders against the Resellers.<sup>15</sup>

### III. THE LIMITS OF THE FTC'S DATA SECURITY ENFORCEMENT POWERS

¶12 The idea that a company has a duty to police *its customers'* data security practices raises a host of unanswered questions. Section A discusses the extent to which the Commission has signaled a policy shift that is intended to apply across industries to all companies that possess sensitive personal information. Section B analyzes whether the FCRA supports the duty to police that the Commission is attempting to create. Section C analyzes the new duty under the GLBA, and Section D analyzes the duty under the Commission's primary enabling statute—the Federal Trade Commission Act.

#### *A. The Intended Scope of the Commission's New Duty*

¶13 There is general uncertainty within the legal community concerning the scope of the duty to police enunciated in the Reseller cases. For example, one legal blog noted that “the FTC's willingness not only to hold a company responsible for security lapses on its own network, but for lapses on its customers' networks, *could broaden the scope of potential liability for financial institutions and other businesses.*”<sup>16</sup> The Consumer Data Industry Association raised the same concern in a comment submitted to the Commission:

The Commissioners' statements [accompanying the Reseller cases] describe some potentially very significant new obligations for firms that provide consumer data to end-users or others. The Commissioners would impose these obligations without any public dialogue or administrative process. Before considering such a major policy shift, the Commission should engage knowledgeable industry participants in a discussion of the import of these obligations.<sup>17</sup>

---

occurred, or should have required such documentation only when they became aware that some of their clients had experienced breaches.

<sup>13</sup> SettlementOne Complaint, *supra* note 8, ¶¶ 13-19; ACRAnet Complaint, *supra* note 8, ¶¶ 11-17; Fajilan Complaint, *supra* note 8, ¶¶ 13-19.

<sup>14</sup> Revised Statement of Commissioner Brill, In Which Chairman Leibowitz and Commissioners Rosch and Ramirez Join, In the Matter of Settlement One Credit Corporation, ACRAnet, Inc. and Fajilan and Associates, FTC File Nos. 082-3208, 098-3088, 092-3089 (Aug. 15, 2011) (emphasis added) *available at* <http://www.ftc.gov/os/2011/08/110819settlementonestatement.pdf>.

<sup>15</sup> Decision and Order, SettlementOne Credit Corp, et al., File No 082-3208 (FTC Aug. 17, 2011) *available at* <http://www.ftc.gov/os/caselist/0823208/110819settlementonedo.pdf>; Decision and Order, ACRAnet, Inc., File No. 092-3088 (FTC Aug. 17, 2011) *available at* <http://www.ftc.gov/os/caselist/0923088/110809acranetdo.pdf>; Decision and Order, Fajilan and Associates, Inc., File No. 092-3089 (FTC Aug. 17, 2011) *available at* <http://www.ftc.gov/os/caselist/0923089/110819statewidedo.pdf>.

<sup>16</sup> Newsletter, Steptoe & Johnson LLP, E-Commerce Law Week, Issue 643 (Feb. 12, 2011) (emphasis added), <http://www.steptoelaw.com/publications-7399.html>; *see also* Report, Bryan Cave, FTC Indicates That Financial Institutions May Be Liable For Customers' Inadequate Security (Feb. 8, 2011), <http://www.bryancave.com/files/Publication/2dd88b6a-3898-4876-bbad-12d47e300a50/Presentation/PublicationAttachment/a618187b-5e50-4e27-81d0-1388462505bf/FTC%20Financial%20Institutions%20Security.pdf>.

<sup>17</sup> Letter from Stuart K. Pratt, President & CEO, Consumer Data Industry Association, to Federal Trade Commission (Mar. 7, 2011) (public comment to Agreement Containing Consent Order, ACRAnet, Inc. File No. 092-3088), *available at* <http://www.ftc.gov/os/comments/acranet/00018-58217.pdf>.

¶14 The general uncertainty about the scope of the Commission's policy is due primarily to three factors.

¶15 First, as noted in the Consumer Data Industry Association's comment, the statement issued by the four Commissioners can be read as indicating that a majority of the Commission believes that "all of those in the chain of handling consumer data"—not just companies that issue credit reports—can be held "responsible for downstream data protection failures."<sup>18</sup>

¶16 Second, the press release that accompanied the announcement of the Reseller cases contained a statement from the Director of the Commission's Bureau of Consumer Protection, David Vladeck, that also implies that the obligation to police one's customers applies to all "companies," not simply to resellers:

"These cases should send a strong message that *companies giving their clients online access to sensitive consumer information* must have reasonable procedures to secure it . . . . Had these three companies taken adequate steps to ensure the use of basic computer security measures, they might have foiled the hackers who wound up gaining access to extensive personal information in the consumer reporting system."<sup>19</sup>

¶17 The Director's statement was widely picked up by the media and re-circulated within the data security community.<sup>20</sup>

¶18 Finally, the complaints issued in the Reseller cases also signal the Commission's belief that a duty-to-police extends beyond the credit reporting industry. The Commission's staff encourages companies to view complaints that allege violations of the FTC Act as signaling that the Commission has adopted a principle or policy that extends beyond a specific industry. For example, a recent post on the FTC's business-focused website contains the following cautionary message to businesses:

Although some FTC rules apply only to certain industries, most lawsuits allege violations of Section 5 of the FTC Act, the federal law broadly outlawing unfair or deceptive acts or practices. That's why savvy marketers of widgets pay attention to FTC cases involving whatzits and whaddayacallems . . . it's wise to look at the big picture – and not just at legal developments directly affecting your business.<sup>21</sup>

¶19 Not surprisingly, practitioners carefully monitor the Commission's complaints to gauge policy shifts. For example, a complaint that alleges that a specific act violates only the FCRA signals that the Commission is concerned only with the practice as it relates to Consumer Reporting Agencies (CRAs). If the same complaint alleges a GLBA violation, the inclusion of the GLBA count signals the Commission's belief that any company governed by the GLBA may be liable for committing a similar act. Similarly, a complaint that also includes the FTC Act signals a belief that any company governed by the FTC Act (which includes the majority of all companies in the United States) may be liable for committing a similar act. In this case, the Commission went out of its way to allege that the Resellers' failure to police their customers violated the FCRA, the GLBA, *and* the FTC Act.

<sup>18</sup> Revised Statement of Commissioner Brill, In Which Chairman Leibowitz and Commissioners Rosch and Ramirez Join, In the Matter of Settlement One Credit Corp., ACRAnet, Inc. and Fajilan and Assocs., FTC File Nos. 082-3208, 098-3088, 092-3089 (Aug. 15, 2011) *available at* <http://www.ftc.gov/os/2011/08/110819settlementonstatement.pdf>.

<sup>19</sup> Press Release, Federal Trade Commission, Credit Report Resellers Settle FTC Charges; Security Failures Allowed Hackers to Access Consumers' Personal Information (Feb. 3, 2011) (emphasis added), *available at* <http://www.ftc.gov/opa/2011/02/settlement.shtm>.

<sup>20</sup> See The New New Internet, *FTC Slams Companies for Failure to Adopt Cybersecurity Measures*, THE NEW NEW INTERNET (Feb. 4, 2011), <http://www.thenewnewinternet.com/2011/02/04/ftc-slams-companies-for-failure-to-adopt-cybersecurity-measures/>; Grant Gross, *FTC Settles Complaints Against Credit Report Resellers*, PC WORLD (Feb. 3, 2011) [http://www.pcworld.com/businesscenter/article/218662/ftc\\_settles\\_complaints\\_against\\_credit\\_report\\_resellers.html](http://www.pcworld.com/businesscenter/article/218662/ftc_settles_complaints_against_credit_report_resellers.html).

<sup>21</sup> Lesley Fair, Sr. Staff Attorney, FTC Bureau of Consumer Protection, *Widgets, Whatzits, and Whaddayacallems*, BUSINESS CENTER BLOG (Aug. 30, 2011), <http://business.ftc.gov/blog/2011/08/widgets-whatzits-and-whaddayacallems>.

*B. The FCRA Does Not Impart a Duty Upon CRAs to Police Their Customers*

¶20 The Commission received fifteen comments from members of the credit reporting industry. Each of these comments questioned whether there was any “basis in the FCRA” to “hold resellers responsible for the potential failures of independent third parties to protect consumer data.”<sup>22</sup>

¶21 The only provision of the FCRA that expressly addresses data security is the requirement, added as part of the Fair and Accurate Credit Transactions Act of 2003, that companies properly dispose of the consumer information that they handle.<sup>23</sup> Nonetheless, starting in 2006 with its enforcement action against ChoicePoint, the FTC has interpreted the FCRA as requiring that companies prevent identity theft by taking reasonable efforts to verify the identity of users prior to furnishing consumer reports.<sup>24</sup>

¶22 According to the FTC, the Resellers failure to police their customers violated two provisions of the FCRA—Sections 604 and 607(a).

¶23 Section 604 permits CRAs to furnish consumer reports only to authorized entities that have a permissible purpose for obtaining a report. According to the FTC, the Resellers violated the section when the hackers obtained copies of the consumer reports because the “hackers . . . did not have a permissible purpose to obtain” them.<sup>25</sup> Taken at face value, the FTC’s allegation suggests that a CRA is strictly liable anytime an unauthorized individual obtains a consumer report that was created by the CRA. Section 604, does not, however, confer strict liability on CRAs—a point that the FTC concedes.<sup>26</sup> To the contrary, the section states that CRAs must only have a “reason to believe” that the person requesting a credit report has an authorized purpose. Based upon the facts alleged in the Reseller complaints, it seems fairly clear that the Resellers’ legitimate business customers—not the hackers—requested that the Resellers provide them with credit reports. Furthermore, those clients requested the reports for a purpose that the FCRA expressly recognizes as legitimate—to determine consumers’ eligibility for credit. The hackers appeared to gain access to the reports *after* they had been legitimately requested by the Resellers’ customers.<sup>27</sup> As a result, not only did the Resellers have a reason to believe that the requesting entity had a legitimate purpose—the requesting entity did, in fact, have such a reason.

¶24 Section 607 requires that CRAs “maintain reasonable procedures” to prevent furnishing consumer reports to entities who are not authorized under the Act. The FTC alleged that policing a customer’s data security practices constitutes the type of reasonable procedure contemplated under the statute. The FTC’s interpretation disregards the fact that Section 607 specifies the types of procedures contemplated under the statute, and contemplates different standards for CRAs with respect to “prospective users” and “new prospective users” of credit reports:

Every consumer reporting agency shall maintain reasonable procedures designed to avoid violations of sections 605 and to limit the furnishing of consumer reports to the purposes

<sup>22</sup> The Commission received 17 comments to the proposed settlement, 15 of which were submitted by industry members and were substantively identical. *See, e.g.*, Letter from Heather Russell-Schroeder, President, Credit Bureau of Council Bluffs, Inc., to Federal Trade Commission (Mar. 7, 2011), *available at* <http://www.ftc.gov/os/comments/acranet/552781-00014-58195.pdf>.

<sup>23</sup> 15 U.S.C. §§ 1681b, 1681w (2010); *see also* FTC Disposal Rule, 16 C.F.R. 682.1, *et seq.* (2005).

<sup>24</sup> Section 604 of the FCRA permits CRAs to furnish consumer reports only under the circumstances enunciated within the statute and “no other.” 15 U.S.C. § 1681b(a) (2010). The FTC has interpreted this language in several enforcement actions as establishing a duty of reasonableness to verify and authenticate users, and assess whether users have a permissible purpose. *See* Complaint ¶ 13, *United States v. ChoicePoint Inc.*, No. 1:06-cv-0198 (N.D. Ga. Jan. 30, 2006) [hereinafter *ChoicePoint Complaint*]; Complaint ¶¶ 17-23, *United States v. Rental Research*, No. 09-cv-00524 (D. Minn. Mar. 5, 2009).

<sup>25</sup> SettlementOne Complaint, *supra* note 8, ¶ 15.

<sup>26</sup> *See* Letter from FTC to Individual Business Commenters (Aug. 17, 2011), *available at* <http://www.ftc.gov/os/caselist/0823208/110819individualbusinesscommenters.pdf>.

<sup>27</sup> It appears from the complaints that the FTC does not allege that the hackers ordered reports from the Resellers themselves. To the contrary, the complaints admit that the reports were ordered from the business clients, and that they were ordered for the purpose of verifying consumer eligibility for credit. Rather, in most situations the hackers accessed the reports *after* the reports had been sent to the customers (i.e., they accessed a copy of the reports on the customers’ networks, not a copy on the Resellers’ networks). In a few instances they accessed archived versions of the reports that existed on the Resellers’ networks by using a business customer’s account credentials. *See* SettlementOne Complaint, *supra* note 8, ¶ 10.

listed under section 604 of this title. These procedures shall require that *prospective users of the information identify themselves, certify the purposes for which the information is sought and certify that the information will be used for no other purpose.* Every consumer reporting agency shall make a reasonable effort to *verify the identity of a new prospective user and the uses certified by such prospective user prior to furnishing such user a consumer report.* No consumer reporting agency may furnish a consumer report to any person if it has reasonable grounds for believing that the consumer report will not be used for a purpose listed in section 604.<sup>28</sup>

¶25 Simply put, for “new prospective users” a CRA must do two things: (1) verify the identity of the new user, and (2) verify the use certified by the new user. For “prospective users” that are not new, such as returning customers, a CRA must require the customer to (1) identify themselves, (2) certify the purpose for which the information is sought, and (3) certify that the information will be used for no other purpose. Whether or not a customer is a “new prospective user” or simply a “prospective user” nothing within Section 607 contemplates that CRAs must verify the adequacy of their customers’ data security.

¶26 It appears that the FTC is trying to interpret the obligation that a credit reporter “verify the identity” of its customer as implicitly requiring that a credit reporter take steps to make sure that its customers are unlikely to become victims of a hacking event. In other words, the FTC may be trying to say that the Resellers had an obligation to prevent the hackers from gaining the account credentials of the Resellers’ business customers, and from using those account credentials to impersonate a business customer in order to view the credit reports that the business customer had ordered in the previous ninety days.

¶27 Such an interpretation would blur Section 607’s distinction between a “prospective user” and a “new prospective user.” While it is clear that a CRA must verify the identity of a new customer, the section does not require that CRAs verify the identity of existing customers.<sup>29</sup> Section 607 only requires that CRAs make existing customers “identify themselves” at the time that they request a credit report. The FTC did not allege that the Resellers failed to require their returning customers to identify themselves. To the contrary, the Resellers had assigned their customers unique logins and passwords for the very purpose of requiring that their customers identify themselves when requesting information (or when viewing information requested in the past).

¶28 The FTC also alleged that the Resellers violated Section 607 because “they had reasonable grounds for believing that the reports would not be used for a permissible purpose.”<sup>30</sup> It is not exactly clear from the complaints what information the Resellers received that could have placed them on notice that their clients had been the victims of data security breaches, or that their clients’ credentials had been stolen and might be used to access the Resellers’ credit reports. While receipt of such information might very well constitute a violation of Section 607, Section 607 does not explicitly support an affirmative duty to police business customers when a company has not received any information that suggests that reports will be used for impermissible purposes.

### *C. The GLBA Does Not Impart a Duty Upon Financial Institutions to Police Their Customers*

¶29 Congress passed GLBA in 1999. Among other things, GLBA imposed a duty upon financial institutions to “protect the security and confidentiality” of their customers’ nonpublic personal information and authorized the federal banking agencies and the FTC to establish “appropriate standards” to guide the financial institutions within their respective jurisdictions.<sup>31</sup>

¶30 In 2001 the federal banking agencies issued joint Interagency Guidelines Establishing Standards for Safeguarding Customer Information (the “Interagency Guidelines”) that addressed how the

<sup>28</sup> 15 U.S.C. §1681e(a) (2011) (emphasis added).

<sup>29</sup> This factual difference distinguishes the Reseller cases from prior Commission actions such as *Choicepoint* where the Commission alleged that the CRA failed to “verify the identity of . . . new prospective user[s].” *ChoicePoint Complaint*, *supra* note 24, ¶ 13 (emphasis added).

<sup>30</sup> *SettlementOne Complaint*, *supra* note 8, ¶ 17.

<sup>31</sup> 15 U.S.C. § 6801(a)–(b) (1999).

entities under their jurisdiction should comply with GLBA. Among other things, the Interagency Guidelines suggest that financial institutions “identify reasonably foreseeable internal and external threats” to customer information that could result in “unauthorized disclosure,” and that they design a written information security program to address the “identified risks.”<sup>32</sup> The Interagency Guidelines also ask financial institutions to require their service providers to implement similar security measures.<sup>33</sup>

¶31 The following year the FTC issued its own “Safeguards Rule,” which it described as an attempt to “mirror[]” the requirements of the Interagency Guidelines.<sup>34</sup> As with the Interagency Guidelines, the Safeguards Rule requires financial institutions to (1) adopt a written information security program, (2) identify “reasonably foreseeable internal and external risks” to customer information that could result in “unauthorized disclosure,” and (3) “design and implement information safeguards” to control, test, and monitor those risks.<sup>35</sup> The Safeguards Rule also requires financial institutions to take reasonable steps when selecting service providers, such as requiring “service providers by contract to implement and maintain” similar safeguards.<sup>36</sup>

¶32 The FTC’s reliance on the Safeguards Rule in the Reseller cases seems to imply that financial institutions must identify reasonably foreseeable “internal and external risks” not only to their own systems and networks, but also to the systems and networks of their customers. The FTC’s interpretation, however, has little support within the text or intended purpose of the Interagency Guidance and the Safeguards Rule for three reasons.

¶33 First, at the time that the Interagency Guidelines and the Safeguards Rule were promulgated, the banking agencies and the FTC made clear that the purpose of the risk assessment was to make sure that financial institutions remediated risks to the financial institutions’ own systems. For instance, the Interagency Guidelines state “[y]ou must consider whether the following security measures *are appropriate for you* and, if so, adopt those measures you conclude are appropriate.”<sup>37</sup> Similarly, the FTC explained in its comments to the Safeguards Rule that a financial institution is required to consider risks “in each area of *its* operations.”<sup>38</sup>

¶34 Second, the banking agencies and the FTC specified that financial institutions would police one category of third parties—service providers. This obligation was not hinted at or implied. Rather, the Interagency Guidelines and the Safeguards Rule dedicated an entire section to “service providers.”<sup>39</sup> After the promulgation of the Safeguards Rule, the FTC identified service providers as the only category of third parties for which a financial institution had a duty to monitor. The FTC stated in a compliance document provided to businesses that “[i]n addition to developing their own safeguards, financial institutions are responsible for taking steps to ensure that their affiliates and service providers safeguard customer information in their care.”<sup>40</sup>

¶35 Third, the policy rationale for requiring financial institutions to police service providers simply does not apply to the policing of customers. Service providers are selected by financial institutions to perform functions that the financial institution could, in theory, perform internally. As the banking agencies noted in their comments to the Interagency Guidelines, when a financial institution decides to outsource a function to a third party, the financial institution is choosing to “creat[e] additional

<sup>32</sup> Interagency Guidelines, 66 Fed. Reg. 8,640 § III(B)(1), (C) (Feb. 1, 2001).

<sup>33</sup> *Id.* § III(C)–(D).

<sup>34</sup> Safeguards for Safeguarding Customer Information, 67 Fed. Reg. 36,484 (Mar. 23, 2002).

<sup>35</sup> 16 C.F.R. § 314.4 (b)–(c) (2002).

<sup>36</sup> *Id.* § 314.4 (d)(2).

<sup>37</sup> Interagency Guidelines, 66 Fed. Reg. at 8,640 (emphasis added) (Feb. 1, 2001).

<sup>38</sup> 67 Fed. Reg. at 36,489 (emphasis added).

<sup>39</sup> 16 C.F.R. § 314.4(d)(1)–(2); Interagency Guidelines, 66 Fed. Reg. at 8,640.

<sup>40</sup> Compliance Document, Federal Trade Commission, Financial Institutions and Customer Information: Complying with the Safeguards Rule (April 2006), <http://business.ftc.gov/documents/bus54-financial-institutions-and-customer-information-complying-safeguards-rule.pdf>.

risks to the security and confidentiality of the information” by disclosing it to the service provider.<sup>41</sup> As the financial institution creates the risk, the financial institution must take steps to mitigate the risk. In contrast, when a customer (whether a business or an individual) retains a financial institution, the financial institution is not “creating” a risk. While a financial institution could theoretically refuse to deal with the customer, it has not chosen or selected the customer; the customer has chosen the institution.

¶36 Even if the Resellers had a duty to police their customers, the banking agencies have made clear that when a financial institution deals with another financial institution it “may take into account the fact that the correspondent bank is itself a financial institution that is subject to security standards under section 501(b) [of GLBA] when it determines the appropriate level of oversight . . . .”<sup>42</sup>

¶37 Most of the Resellers’ customers were financial institutions (i.e., mortgage brokers), who were themselves subject to the Safeguards Rule, and, as a result, had a statutory obligation to review their own systems to identify reasonably foreseeable internal and external risks and to take steps to control, test, and monitor those risks.<sup>43</sup> In light of the fact that their customers were subject to GLBA and the Safeguards Rule, even if the Resellers had a duty to police them, that duty could arguably be discharged with a minimum of oversight.

*D. The “Unfairness Authority” of the Federal Trade Commission Act Does Not Impart Upon All Businesses a Duty to Police Their Customers*

¶38 In September of 2005, the FTC brought an enforcement action against BJ’s Wholesale Club, Inc. for its failure to take “reasonable and appropriate measures to secure” personal information.<sup>44</sup> This was the first time that the FTC had premised a data security enforcement action only upon the unfairness authority afforded to the Commission under Section 5 of the FTC Act.<sup>45</sup> Since then, the FTC has proceeded against at least five other companies for data security breaches using only its unfairness authority.<sup>46</sup>

¶39 The scope of the Commission’s “unfairness jurisdiction” under Section 5 has long been controversial. Indeed, fears that the unfairness authority afforded the Commission too much discretion prompted Congress to consider revoking the authority in the 1980s. In response to that threat, and in recognition of the fact that the bounds of the unfairness authority were “not immediately obvious” to Congress, businesses, or the legal profession, the Commission issued its “Policy Statement on Unfairness” to provide a “concrete framework” for how the Commission would apply its authority.<sup>47</sup> The three-part test established in the Unfairness Statement, later codified by Congress, permits the use of unfairness authority only where there is (1) “substantial” consumer

<sup>41</sup> Interagency Guidelines, 66 Fed. Reg. 8,619.

<sup>42</sup> *Id.*

<sup>43</sup> The FTC has issued specific guidance to the mortgage broker industry informing them that they are “subject to the FTC’s enforcement authority, its Privacy Rule, and its Safeguards Rule.” Guidelines, Federal Trade Commission, Additional Frequently Asked Questions About the Privacy Regulation and Mortgage Brokers (Jan. 2003), <http://www.ftc.gov/privacy/glbact/glb-faq-more.htm>.

<sup>44</sup> Complaint, In the Matter of BJ’s Wholesale Club, Inc., FTC Case No. C-4148, *available at* <http://www.ftc.gov/os/caselist/0423160/092305comp0423160.pdf>

<sup>45</sup> Prior to 2005, the Commission had taken inconsistent positions concerning its ability to use unfairness to pursue a claim that a company had used inadequate security. *See* FEDERAL TRADE COMMISSION, PRIVACY ONLINE: FAIR INFORMATION PRACTICES IN THE ELECTRONIC MARKETPLACE: A REPORT TO CONGRESS 34 (May 2000), *available at* <http://www.ftc.gov/reports/privacy2000/privacy2000.pdf> (stating that the Commission lacked authority to require firms to adopt information practices if the firm did not make a deceptive statement about its practices).

<sup>46</sup> *See* Complaint, DSW Inc., No. C-4157 (FTC Mar. 7 2006), *available at* <http://www.ftc.gov/os/caselist/0523096/0523096c4157DSWComplaint.pdf>; Complaint, CardSystems Solutions, Inc., No. C-4168 (FTC Sept. 5, 2006), *available at* <http://www.ftc.gov/os/caselist/0523148/0523148CardSystemscomplaint.pdf>; Complaint ¶ 13, Reed Elsevier Inc., No. C-4226 (FTC July 29, 2008), *available at* <http://www.ftc.gov/os/caselist/0523094/080801reedcomplaint.pdf>; Complaint ¶ 11, TJX, No. C-4227 (FTC July 29, 2008), *available at* <http://www.ftc.gov/os/caselist/0723055/080801tjxcomplaint.pdf>; Complaint, Dave & Buster’s, Inc., No. C-4291 (FTC May 20, 2010), *available at* <http://www.ftc.gov/os/caselist/0823153/100608davebusterscmpt.pdf>; Complaint, BJ’s Wholesale Club, Inc., No. C-4148 (FTC Sept. 20, 2005), *available at* <http://www.ftc.gov/os/caselist/0423160/092305comp0423160.pdf>; *see also*

<sup>47</sup> FTC Policy Statement on Unfairness, 1, *appended to* In the Matter of Int’l Harvester Co., 104 F.T.C. 949, 1070 (1984).

injury, (2) the injury is not “outweighed by countervailing benefits to consumers or to competition,” and (3) the injury is “not reasonably avoidable by consumers themselves.”<sup>48</sup> It is highly doubtful that the practice about which the Commission complains—a failure to police a company’s customers by monitoring their data security practices—meets any of these criteria.

¶40 With regard to the first part of the test, the statement of Commissioners Brill, Leibowitz, Rosch, and Ramirez emphasizes that the “significant impact and cost of identity theft are well documented.” The Commissioners point to a report that indicates that in 2005, 25% of victims of identity theft incurred more than \$1,000 in out-of-pocket expenses and others incurred “non-economic harm” including denial of credit, harassment, and loss of time.<sup>49</sup> While nobody disputes that identity theft has a significant negative effect on consumers and on the economy, that fact alone does not support the use of unfairness authority. The unfairness analysis asks a very specific question—whether *the practice of which the Commission complains* has a “substantial” negative impact on consumers. The practice that the Commission complains about in the Reseller cases is not the theft of a consumer’s identity. Rather it is the failure of a company to take steps to make sure that its customers have sufficient security systems to prevent hackers from gaining access to their networks.

¶41 The Commission did not cite any evidence demonstrating that this failure to police has a “substantial” negative impact on consumers. For instance, the Commission did not demonstrate that a substantial percentage of data breaches occur when hackers gain access to a customer’s machines (as opposed to gaining access to the data holder’s machines). Nor did the Commission discuss (let alone demonstrate) whether there is a causal connection between hacking events and identity theft. Although it may seem like such a connection might be taken for granted, even federal agencies have substantial questions concerning the extent to which data breaches actually lead to identity theft.<sup>50</sup> In summary, the Commission’s conclusion appears to rely on at least three layers of inferential reasoning: (1) customers generally do not employ adequate security measures themselves, (2) a substantial number of hacking events target customers as opposed to up-stream data providers, and (3) those hacking events lead to actual identity theft.<sup>51</sup>

¶42 With regard to the second part of the three-part consumer injury test, the Commission must take into account the “various costs that a remedy would entail” when weighing whether consumer injury justifies the use of unfairness authority.<sup>52</sup> Among other things, these costs include “the burdens on society in general in the form of increased paperwork, [and] increased regulatory burdens on the flow of information.”<sup>53</sup> It is unclear how much of a burden the steps that the Commission alleges that the Resellers should have taken, such as requiring that “end user clients submit . . . documentation demonstrating that the client’s computer systems were virus free, would impose.<sup>54</sup> These costs, and

<sup>48</sup> 15 U.S.C. 45(n) (2006); *see also* FTC Policy Statement on Unfairness, *supra* note 47, at 3.

<sup>49</sup> Statement of Commissioner Brill, in Which Chairman Leibowitz and Commissioners Rosch and Ramirez Join, *available at* <http://www.ftc.gov/os/caselist/0823208/110203settlementonstatement.pdf> (citing SYNOVATE, 2006 IDENTITY THEFT SURVEY REPORT 37 (2007), *available at* <http://www.ftc.gov/os/2007/11/SynovateFinalReportIdtheft2006.pdf>).

<sup>50</sup> *See* UNITED STATES GOVERNMENT ACCOUNTABILITY OFFICE REPORT TO CONGRESSIONAL REQUESTERS, PERSONAL INFORMATION: DATA BREACHES ARE FREQUENT, BUT EVIDENCE OF RESULTING IDENTITY THEFT IS LIMITED; HOWEVER, THE FULL EXTENT IS UNKNOWN (2007), *available at* <http://www.gao.gov/new.items/d07737.pdf>. The GAO Report analyzed the 24 largest breaches reported in the media from January 2000 through January 2005 and found that only three of the breaches included evidence of resulting fraud on existing accounts, and only one of the breaches included evidence of unauthorized creation of new accounts. Even in the Reseller cases it is unclear whether there was any evidence of actual identity theft. In addition, federal courts have dismissed several private lawsuits against companies that have experienced data breaches based upon the inability of plaintiffs to prove injury, or to demonstrate a legitimate fear of future injury. *See, e.g.*, *Pisciotta v. Old Nat'l Bancorp*, 499 F.3d 629, 639 (7th Cir. 2007) (affirming dismissal for failure to allege injury-in-fact); *Reilly v. Ceridien Corp.*, No. 10-5142, 2011 U.S. Dist. LEXIS 17833 at \* 13 (D.N.J. Feb. 22, 2011) (dismissing suit for failure to allege injury-in-fact).

<sup>51</sup> The Unfairness Statement makes clear that the Commission will not exercise its unfairness jurisdiction based upon “speculative” harm. FTC Policy Statement on Unfairness, *supra* note 47, at 3.

<sup>52</sup> *Id.*

<sup>53</sup> *Id.*

<sup>54</sup> These steps include requiring that “end user clients submit any documentation demonstrating that the client’s computer systems were virus free and otherwise properly protected . . . .” SettlementOne Complaint, *supra* note 8, ¶ 11. but it is clear that the administrative burden for businesses with thousands, or tens of thousands, of business and consumer customers would be enormous

the potential delay that requesting and obtaining such documentation might cause, could conceivably be significant particularly if the reseller had thousands, or tens of thousands, of clients.

¶43 The third factor of the three-part test makes it virtually impossible to apply a duty to police customers against at least one category of businesses: retailers whose customers are individual consumers. There can be little doubt that a retailer's customers could avoid the type of harm described by the Commission by simply deciding for themselves to take basic security measures, such as installing off-the-shelf antivirus software and firewalls.<sup>55</sup> It also raises serious questions concerning whether the Commission could apply a duty to police customers in precisely the scenario presented in the Reseller cases: a situation in which a business's corporate customer was, itself, selected by an end-consumer. In such a situation, the end-consumer could avoid injury by inquiring about the security policies of the company with whom they have a relationship, or only doing business with companies that represent themselves as having high security standards. As J. Howard Beales, III recognized while he was Director of the Bureau of Consumer Protection, under the third factor of the unfairness test, "if consumers could have made a different choice, but did not, the Commission should respect that choice."<sup>56</sup> To the extent that a large number of consumers choose not to avoid the injury presents "a strong argument for consumer education," not law enforcement, under the Commission's unfairness authority.<sup>57</sup>

## CONCLUSION

¶44 While the Commission has announced over thirty data security consent orders against businesses since the Commission initiated its data security program ten years ago, the Commission has not litigated a single case.<sup>58</sup> Instead, the Commission has left a trail of consent orders which signal to the consumer protection community and to the companies that collect, share, or use data, how the Commission interprets companies' obligation to secure data. The new Reseller cases raise significant questions concerning the Commission's current interpretation of the data security laws. If the Commission attempts to apply the concepts of the Reseller cases broadly, and practitioners and companies decide to challenge that interpretation, the Commission may have difficulty defending its jurisprudence-by-acclamation in court.

---

<sup>55</sup> This factor may make it equally impossible to apply the duty to police one's customers against companies, like the Resellers, whose clients are businesses which themselves have a direct relationship with individual consumers. In such situations, an individual consumer could avoid the type of harm described by the Commission by simply choosing to require that the business with whom he deals (i.e., the mortgage brokers) enact appropriate data security safeguards.

<sup>56</sup> J. Howard Beales, III, *The FTC's Use of Unfairness Authority: Its Rise, Fall, and Resurrection*, 22 J. OF PUB. POLICY & MARKETING 3 (2003), available at <http://www.ftc.gov/speeches/beales/unfair0603.shtm>.

<sup>57</sup> *Id.*

<sup>58</sup> A list of the Commission's data security related enforcement actions can be found at [http://www.ftc.gov/privacy/privacyinitiatives/promises\\_enf.html](http://www.ftc.gov/privacy/privacyinitiatives/promises_enf.html).