Statement of Commissioner Brill, In Which Chairman Leibowitz and Commissioners Rosch and Ramirez Join
In the Matter of SettlementOne Credit Corporation, et al.
In the Matter of ACRAnet, Inc.
In the Matter of Fajilan and Associates, et al.
(Revised 8.15.2011)

The respondents in these three matters are resellers of consumer reports who allegedly failed to take reasonable measures to protect sensitive consumer credit information. We fully support staff's work in these matters. We write separately to emphasize that in the future we will call for imposition of civil penalties against resellers of consumer reports who do not take adequate measures to fulfill their obligations to protect information contained in consumer reports, as required by the Fair Credit Reporting Act ("FCRA").

The allegations indicate that respondents in these three matters treated their legal obligations to protect consumer information as a paper exercise. According to the complaint, respondents provided only a cursory review of security measures. Thereafter, respondents took no further action to ensure that their customers' security measures adequately protected the information in consumer reports. Nor did they provide training on security measures to end users. Even after discovering security breaches that should have alerted them to problems with the data security of some customers, respondents failed to implement measures to check the security practices of other clients.

The FCRA requires respondents to take reasonable measures to ensure that consumer reports are given only to entities using the reports for purposes authorized by the statute.[1] The complaints alleged that, as a result of respondents' failure to comply with the FCRA, nearly 2,000 credit reports were improperly accessed. There is no doubt that such unauthorized access can result in grave consumer harm through identity theft.

The significant impact and cost of identity theft are well documented. Although reports regarding the impact of identity theft do not always agree on specific figures, they do reveal tremendous economic and non-economic consequences for both consumers and the economy. The Commission itself issued reports in both 2003[2] and 2007.[3] Our 2007 report estimated that in 2005 alone 8.3 million consumers fell victim to identity theft. We found that 1.8 million of those victims had new accounts opened in their names. One-quarter of the "new account victims" incurred more than $1,000 in out-of-pocket expenses and five percent spent 1,200 hours dealing with the consequences of the theft. The report concluded that total losses from identity theft in 2006 totaled $15.6 billion. Beyond these financial impacts, we also identified non-economic harm to victims in many forms: denial of new credit or loans, harassment from collection agencies, the loss

[1] 15 U.S.C. § 1681b; 15 U.S.C. § 1681e(a).
[2] Fed. Trade Comm'n, Identity Theft Survey Report (2003), available at http://www.ftc.gov/os/2003/09/synovatereport.pdf
[3] Fed. Trade Comm'n, 2006 Identity Theft Survey Report (2007), available at http://www.ftc.gov/os/2007/11/SynovateFinalReportIDTheft2006.pdf

of the time involved in resolving the problems, and being subjected to criminal investigation. In view of the hardships and costs brought on by identity theft, measures to prevent it must be rigorously enforced.

While we view the breaches in these cases with alarm, we 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.[4] 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. In the future, we should not hesitate to use our authority to seek civil penalties under the FCRA[5] to make the protection of consumer data a top priority for those who profit from its collection and dissemination.

[4] The Commission has previously taken action where a credit reporting agency failed to adequately screen purchasers of consumer credit information. For instance, in United States v. ChoicePoint, Inc., 06-CV-0198 (N.D. Ga. Oct. 19, 2009), the Commission alleged that the failure to screen customers led to the sale of 160,000 credit reports to identity thieves posing as customers of ChoicePoint.

[5] The Fair Credit Reporting Act authorizes the Commission to seek civil penalties for violations of the Act. 15 U.S.C. § 1681s(a)(2)(A).