epic.org

In the Matter of Reed Elsevier, Inc. and Seisint, Inc. Consent Order
FTC Docket No. 052-3094

In the Matter of The TJX Companies, Inc. Consent Order
FTC Docket No. 072-3055

1718 Connecticut Ave NW
Suite 200
Washington DC 20009
USA
+1 202 483 1140 [tel]
+1 202 483 1248 [fax]
www.epic.org

COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER (EPIC)

EPIC submits the following comments pursuant to the March 27, 2008 notice[1] published by the Federal Trade Commission regarding the Consent Orders entered into by the Commission and 1) The TJX Companies, Inc. ("TJX"); and 2) Reed Elsevier, Inc. and Seisint, Inc. (jointly, "LexisNexis").

We commend the Commission for taking action in these cases. However, the Consent Orders should be revised to better protect consumer privacy through the imposition of civil penalties against TJX and LexisNexis. The Commission has imposed civil penalties for data breaches in the past, and such penalties have provided incentives for companies to better safeguard sensitive consumer data. EPIC encourages the Commission to impose civil penalties as terms of each Consent Order.

The Data Breaches

TJX is a discount retailer with more than 2,500 stores worldwide. Since approximately 2005, TJX failed to use reasonable security measures to prevent unauthorized access to personal information on its computer networks. A criminal exploited TJX's unreasonably weak security policies, and obtained tens of millions of credit and debit payment card numbers that consumers used at TJX's stores. Other personal information concerning approximately 455,000 TJX consumers was also unlawfully obtained. TJX's unreasonable security practices caused the data breach, and resulted in tens of millions of dollars in claims for fraudulent credit card charges, as well as the cancellation and reissuance of millions of cards.[2]

---

[1] U.S. Federal Trade Commission, *Agency Announces Settlement of Separate Actions Against Retailer TJX, and Data Brokers Reed Elsevier and Seisint for Failing to Provide Adequate Security for Consumers' Data*, March 27, 2008, available at: http://www.ftc.gov/opa/2008/03/datasec.shtm.

[2] *In the Matter of The TJX Companies, Inc.*, FTC Docket No. 072-3055 (FTC 2008) (Complaint), available at: http://www.ftc.gov/os/caselist/0723055/080327complaint.pdf.

LexisNexis, a data broker, collects and stores information about millions of consumers, including names, current and prior addresses, dates of birth, drivers license numbers, and Social Security numbers. From approximately late 2004 through mid-2005, LexisNexis failed to use reasonable security measures to prevent unauthorized access to its databases. Criminals exploited these security failures, and obtained sensitive information about at least 316,000 consumers. Criminals then used the information to activate credit cards, open new accounts, and make fraudulent purchases.[3]

The Consent Orders

The Consent Orders negotiated by the Commission broadly require that TJX and LexisNexis implement comprehensive information security programs. The Consent Orders also require that the companies obtain biennial independent audits of their respective information security programs for twenty years. TJX and LexisNexis are also required to retain documents related to their information security programs and audits for the previous three to five years throughout the twenty-year period.[4]

We believe that the Consent Orders may result in marginal improvements to TJX and LexisNexis' security and privacy practices. However, information security programs and audits will not safeguard the sensitive consumer data held by TJX and LexisNexis unless the companies have strong practical incentives to vigorously implement their obligations under the Consent Orders. The imposition of substantial civil penalties would provide strong incentives. Furthermore, civil penalties in these matters will provide incentives to other companies who collect and store sensitive consumer data.

The Commission Should Impose Civil Penalties

As set forth above, TJX caused a data breach that led to the compromise of tens of millions of credit/debit card numbers and associated information, as well as the disclosure of information concerning approximately 455,000 consumers. LexisNexis caused a data breach that resulted in the disclosure of approximately 300,000 consumers' personal information (including social security numbers, addresses, and dates of birth), and resulted in substantial financial fraud. TJX and LexisNexis caused these data breaches by failing to provide reasonable and appropriate security for sensitive consumer information stored in their computer systems.

---

[3] *In the Matter of Reed Elsevier, Inc. and Seisint, Inc.*, FTC Docket No. 052-3094 (FTC 2008) (Complaint), available at: http://www.ftc.gov/os/caselist/0523094/080327complaint.pdf.

[4] *In the Matter of The TJX Companies, Inc.*, FTC Docket No. 072-3055 (FTC 2008) (Agreement Containing Consent Order), available at: http://www.ftc.gov/os/caselist/0723055/080327agreement.pdf; *In the Matter of Reed Elsevier, Inc. and Seisint, Inc.*, FTC Docket No. 052-3094 (FTC 2008) (Agreement Containing Consent Order), available at: http://www.ftc.gov/os/caselist/0523094/080327agreement.pdf.

TJX and LexisNexis's actions warrant the imposition of civil penalties as a purely punitive measure. In addition, civil penalties would provide strong incentives for TJX, LexisNexis, and other companies to better safeguard sensitive consumer data in the future. The inclusion of civil penalties in the Consent Orders would send the clear message that serious financial consequences will result if companies fail to protect consumer data in the future.

The Commission previously imposed civil penalties in similar circumstances. In December 2004, EPIC filed a complaint with the Commission against databroker ChoicePoint, Inc. alleging that ChoicePoint's business practices put consumers' privacy at risk.[5] We supplemented the complaint in February 2005.[6] Later that year, the Commission determined that ChoicePoint's failure to employ reasonable security policies compromised the sensitive personal data of more than 163,000 consumers.[7] On January 26, 2006, the Commission announced the settlement of its case against ChoicePoint. Like the TJX and LexisNexis Consent Orders, the ChoicePoint settlement required the company to implement a comprehensive information security program and obtain independent audits of its information security programs for twenty years. Unlike the Consent Orders under consideration in this proceeding, the FTC ChoicePoint settlement also required the company to pay $10 million in civil penalties and $5 million in consumer redress.

The TJX and LexisNexis data breaches were caused by the same type of factors as the ChoicePoint breach: the companies' failures to employ reasonable and appropriate security policies. The TJX and LexisNexis data breaches resulted in the unlawful disclosure of the same type of information as the ChoicePoint breach: sensitive consumer data. The TJX data breach compromised tens of millions of credit card numbers and affected approximately 455,000 consumers – more than double the number of consumers affected by the ChoicePoint breach. The LexisNexis data breach resulted in the disclosure of approximately 300,000 consumers' sensitive personal information – almost twice as many consumers as the ChoicePoint breach.

The similarities are striking between the ChoicePoint data breach on the one hand, and the TJX and LexisNexis breaches on the other. The difference between the financial penalty imposed in the ChoicePoint settlement and the TJX and LexisNexis Consent Orders is equally remarkable. Given the greater severity of the TJX and LexisNexis data breaches, each Consent Order should include civil penalties of at least $10 million – the civil penalty levied in the ChoicePoint settlement.

---

[5] *See generally* EPIC, *EPIC Choicepoint Page*, http://epic.org/privacy/choicepoint/.
[6] *Id.*
[7] U.S. Federal Trade Commission, *ChoicePoint Settles Data Security Breach Charges; to Pay $10 Million in Civil Penalties, $5 Million for Consumer Redress*, January 26, 2006, available at: http://www.ftc.gov/opa/2006/01/choicepoint.shtm.

Conclusion

EPIC asks the Commission to include civil penalties in an amount of not less than $10 million as a term of the Consent Order with TJX. EPIC further asks the Commission to include civil penalties in an amount of not less than $10 million as a term of the Consent Order with LexisNexis. EPIC encourages the Commission to seize this unique opportunity to promote consumer privacy and provide strong incentives for companies to better safeguard sensitive consumer data.

Respectfully submitted,

Marc Rotenberg
EPIC Executive Director

John Verdi
EPIC Staff Counsel

ELECTRONIC PRIVACY INFORMATION CENTER
1718 CONNECTICUT AVE., NW, SUITE 200
WASHINGTON, DC 20009
202-483-1140 (TEL)
202-483-1248 (FAX)

FILED: APRIL 28, 2008