Table of Contents

United States
SECURITIES AND EXCHANGE COMMISSION

Washington, D.C. 20549

FORM 8-K

Current Report
Pursuant to Section 13 or 15(d) of the Securities Exchange Act of 1934

Date of Report (date of earliest event reported):
July 3, 2007

Fidelity National Information Services, Inc.

(Exact name of Registrant as Specified in its Charter)

1-16427
(Commission File Number)

Georgia	58-2606325
(State or Other Jurisdiction of Incorporation or Organization)	(IRS Employer Identification Number)

601 Riverside Avenue
Jacksonville, Florida 32204

(Addresses of Principal Executive Offices)

(904) 854-8100
(Registrant's Telephone Number, Including Area Code)

(Former Name or Former Address, if Changed Since Last Report)

Check the appropriate box below if the Form 8-K filing is intended to simultaneously satisfy the filing obligation of the registrant under any of the following provisions:

o Written communications pursuant to Rule 425 under the Securities Act (17 CFR 230.425)

o Soliciting material pursuant to Rule 14a-12 under the Exchange Act (17 CFR 240.14a-12)

o Pre-commencement communications pursuant to Rule 14d-2(b) under the Exchange Act (17 CFR 240.14d-2(b))

o Pre-commencement communications pursuant to Rule 13e-4(c) under the Exchange Act (17 CFR 240.13e-4(c))

TABLE OF CONTENTS

Table of Contents

Item 7.01 Regulation FD Disclosure

On July 3, 2007, Fidelity National Information Services, Inc. ("FIS") announced that its subsidiary Certegy Check Services, Inc., had learned of the misappropriation of consumer information by a former employee. Further details regarding these events are included in FIS's press release, filed as Exhibit 99.1 to this report and incorporated herein by reference.

Although FIS currently does not believe that it faces any significant liability for consumer or financial fraud, there can be no assurance that this matter will not result in fines or other charges or adversely affect FIS's relationships with the VISA and Master Card issuing organizations, customers or regulators.

This report contains forward-looking statements and is subject to the statements in the section of the incorporated press release titled "Forward Looking Statements."

Item 9.01. Financial Statements and Exhibits.

(d) Exhibits

99.1 Press Release dated July 3, 2007.

Table of Contents

SIGNATURE

Pursuant to the requirements of the Securities Exchange Act of 1934, the registrant has duly caused this report to be signed on its behalf by the undersigned thereunto duly authorized.

Fidelity National Information Services, Inc.

Date: July 3, 2007

By: /s/ Jeffrey S. Carbiener
Name: Jeffrey S. Carbiener
Title: Executive Vice President and
Chief Financial Officer

Table of Contents

EXHIBIT INDEX

Exhibit	Description
99.1	Press Release dated July 3, 2007.

EXHIBIT 99.1

Press Release

For More Information:

Michelle Kersch, 904.854.5043
Senior Vice President
Corporate Communications
Fidelity National Information Services
michelle.kersch@fnis.com

Mary Waggoner, 904.854.3282
Senior Vice President
Investor Relations
Fidelity National Information Services
mary.waggoner@fnis.com

For Immediate Release
Tuesday, July 3, 2007

Fidelity National Information Services Announces
Misappropriation of Consumer Data by Employee of Certegy Check Services Division

Data sold to Marketing Solicitation Companies;
No Fraudulent Activity of Identity Theft Detected

Secret Service and Local Law Enforcement Investigations are Ongoing

JACKSONVILLE, Fla. — Fidelity National Information Services, Inc. (NYSE: FIS), announced today that its subsidiary, Certegy Check Services, Inc. ("Certegy"), a service provider to U.S. retail merchants, based in St. Petersburg, Florida, was victimized by a former employee who misappropriated and sold consumer information to a data broker who in turn sold a subset of that data to a limited number of direct marketing organizations. The incident does not involve any outside intrusion into, or compromise of, Certegy's technology systems.

"As a result of this apparent theft, the consumers affected received marketing solicitations from the companies that bought the data," said Renz Nichols, President of Certegy Check Services. "We have no reason to believe that the theft resulted in any subsequent fraudulent activity or financial damage to the consumer, and we are taking the necessary steps to see that any further use of the data stops."

Background
Certegy maintains bank account information in connection with its check authorization business that helps merchants to decide whether to accept checks as payment for goods and services. In addition, Certegy maintains check and credit card information in connection with its gaming operations that are designed to assist casinos in providing their customers with access to funds.

This theft came to light when one of Certegy's retail check processing customers alerted Certegy to a correlation between a small number of check transactions and the receipt by the retailer's customers of direct telephone solicitations and mailed marketing materials. Certegy launched an immediate investigation and was unable to detect any breach of its security systems and, thereafter, engaged a forensic investigator to validate its findings. Unable to detect any compromise in its firewalls and other system security measures, Certegy requested that the U.S. Secret Service contact the marketing companies in question to trace the source of the data. The Secret Service was able to identify the company supplying the information and, with further assistance from Certegy, determined that the company was owned and operated by a Certegy employee. The employee was a senior level database administrator who was entrusted with defining and enforcing data access rights. To avoid detection, the technician removed the information from Certegy's facility via physical processes; not electronic transmission.

Employee Betrayal
Although the employee was authorized to access the consumer information in order to perform his job responsibilities, the removal and unlawful use of that information were, obviously, outside the scope of his employment and Certegy's knowledge. This unlawful transfer of company information violated the individual's confidentiality commitment to Certegy and is a severe breach of fiduciary duty. As a result, the employee was terminated. Certegy is taking appropriate steps to hold the dismissed employee responsible for his actions.

No Evidence of Fraud
The misappropriated information included names, addresses, and telephone numbers as well as, in many cases, dates of birth and bank account or credit card information. Approximately 2.3 million records are believed to be at issue, with approximately 2.2 million containing bank account information and 99,000 containing credit card information. The company is still investigating the time period over which the misappropriations occurred.

While Certegy's investigation continues, it has seen no evidence that bank account or credit card information was used for anything other than marketing purposes, and is unaware of any instance of identity theft or fraudulent financial activity. Most importantly, Certegy is doing everything possible to ensure that any inconvenience experienced by consumers is minimized.

Immediate Action
Certegy is committed to a disciplined action plan designed to minimize the impact of the misappropriated consumer information, particularly to consumers.

- Certegy has filed a civil complaint in St. Petersburg, Florida against the former employee and the marketing companies believed to have received the misappropriated data seeking retrieval of all consumer information as well as an injunction against any use.

- Certegy has contacted the applicable marketing companies in order to obtain the return of all consumer information.
- Certegy proactively engaged law enforcement and is encouraging immediate prosecution.
- Certegy is in the process of making any required notifications to governing state regulatory agencies.
- Certegy has alerted the nation's three major credit reporting agencies, TransUnion, Equifax and Experian.
- Certegy has notified Visa and MasterCard of the incident.
- Certegy is establishing a procedure for financial institutions to obtain information about their customers' accounts so that they can place them on an active fraud watch.
- Certegy will be personally notifying all affected consumers of this misappropriation, and establishing a toll-free hotline to answer consumer questions.
- Certegy has implemented a fraud watch on its internal systems for those checking accounts that are implicated.
- Certegy continually reviews its security policies, and is taking steps to help prevent future incidents.
- Certegy continues to confirm that there was no financial or identity theft caused by this incident; only the improper use of information for telemarketing and mail solicitations.

Based on the investigation to date, Certegy does not expect that the costs to implement this action plan will materially impact financial results.

Certegy will host a news conference via telephone (800) 289-0544 at 9:30 am ET, Tuesday, July 3, 2007.

Conclusion

Certegy is a conscientious company that takes its responsibility to protect and preserve consumer information very seriously. It carefully selects and screens employee candidates, monitors and supervises employees, and maintains a whistleblower hotline for employees to report fraudulent or criminal activity. Certegy also encourages its employees to report any improper behavior they witness. We regret this unfortunate incident happened despite all of these efforts. Resolving this matter and implementing additional safeguards is the company's highest priority.

"I am extremely proud of the employees and law enforcement officials who are working diligently to uncover the facts in this incident. On behalf of Fidelity National Information Services and our Certegy subsidiary, I want to express my deep sadness and heartfelt apology over this incident," said Lee A. Kennedy, President and Chief Executive Officer, Fidelity National Information Services. "We will do everything possible to ensure no consumer is harmed because of this horrible betrayal."

Forward Looking Statements

This press release contains forward-looking statements that involve a number of risks and uncertainties. Statements that are not historical facts, including statements about our beliefs and expectations, are forward-looking statements. Forward-looking statements are based on

management’s beliefs, as well as assumptions made by, and information currently available to, management. Because such statements are based on expectations and are not statements of fact, actual events and results may differ materially from those projected. We undertake no obligation to update any forward-looking statements, whether as a result of new information, future events or otherwise. The risks and uncertainties which forward-looking statements are subject to include, but are not limited to, the possibility that additional facts are discovered in our continuing investigation and the reactions of consumers, regulators and others to the events described above.