:certegy

Certegy Check Services
100 Second Avenue South, Suite 1100S
St Petersburg, Florida 33701

July 5, 2007

Lauren J. Noether, Bureau Chief
Consumer Protection & Anti Trust
33 Capital Street
Concord, NH 03301

RE: Certegy Check Services, Inc.
100 Second Ave. South
St. Petersburg, FL 33701

Dear Ms. Noether:

Please see attached a hard copy of the faxed documents, which were sent to you yesterday, July 4, 2007. At this time, we estimate the number of New Hampshire residents affected by this matter is six thousand nine hundred thirty-three (6933). We are in the process of resolving a number of incomplete addresses. If, as a result of that process, the number of affected New Hampshire residents' increases significantly, we will notify you of the updated number of residents.

Thank you for your consideration in this matter. Should you have any questions, please contact me at 904-357-1663.

Sincerely

Maria L. Vivas, Esq.
AVP & Division Counsel

:certegy

July 4, 2007

Lauren J. Noether
Bureau Chief, Consumer Protection & Anti Trust
33 Capital Street
Concord, NH 03301

RE: Certegy Check Services, Inc.
100 Second Ave. South
St. Petersburg, FL 33701

Dear Ms. Noether:

We are writing to notify you of a misappropriation of consumer data by an employee of Certegy Check Services, Inc. Please see attached a copy of the press release, along with a copy of the notice to consumers. Experian, TransUnion and Equifax credit bureaus were notified yesterday, July 3, 2007.

The determination of the breach was made late on Wednesday June 27, 2007. At this time, we do not have an actual count of the number of New Hampshire residents who will be affected. However, we wanted to send this notice to you as promptly as possible. Notices will be mailed to the consumers on July 5, 2007 and will be finalized not later than July 12, 2007.

Once the count of New Hampshire residents is available, a follow up letter containing the number will be sent to you.

Should you have any questions, please feel free to call me at 904-357-1663.

Sincerely,

Maria L. Vivas, Esq.

FIDELITY NATIONAL
INFORMATION SERVICES

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 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.
- The company is in the process of making any required notifications to governing state regulatory agencies.
- The company has alerted the nation's three major credit reporting agencies, TransUnion, Equifax and Experian.
- Certegy has notified Visa and MasterCard of the incident.
- The company 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.
- The company 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.

:certegy

July 5, 2007

[Insert Name]
[Insert Address]

Important Information Regarding Account Number Ending in XXXX

Dear [Name]:

Certegy Check Services, Inc. (Certegy), a service provider to U.S. retail merchants, was recently victimized by an employee who wrongfully removed 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. For your background, Certegy provides check authorization services to U.S. retail merchants and also provides certain credit card-related services to the gaming industry. As a result of our investigation, Certegy believes that information regarding the above-indicated account was included in the misappropriated information.

While Certegy's investigation into this incident continues, Certegy has seen no evidence that your information has been used for anything other than marketing purposes, and is unaware of any instance of identity theft or fraudulent financial activity. From our investigation thus far, it appears that an employee wrongfully removed 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 information included certain checking account and credit/debit card data, including name, address, telephone number, account number, expiration date (for credit/debit cards) and, in some checking account cases, transactional data and date of birth. The employee was acting without Certegy's knowledge and in violation of his confidentiality agreement with Certegy, and the incident does not arise out of any external intrusion into, or compromise of, Certegy's technology systems.

As you might expect, the employee was terminated upon Certegy learning of his actions. Certegy promptly investigated this incident to ensure that any inconvenience experienced by you is minimized. In particular, Certegy:

- Contacted law enforcement officials to assist in the investigation and has continued to work closely with them on the investigation and a possible criminal prosecution;
- Contacted the applicable marketing companies in order to obtain the return of all consumer information;
- Initiated legal action to guard against any future misuse of the consumer information;
- Contacted the three nationwide credit reporting agencies to alert them to this incident; and
- Implemented a fraud watch on Certegy's internal systems for those checking accounts that were impacted.

Again, Certegy has seen no evidence of identity theft or fraudulent financial activity involving your account, but we strongly recommend that you closely monitor your account and, if you notice any unauthorized activity, promptly contact your financial institution. Periodic review of your credit report can also help identify suspicious activity at an early stage. On the reverse side of this letter is a Reference Guide giving you more information on identity theft, how to report it and how to protect yourself. You can learn more about this matter by visiting the Certegy web site at www.certegy.com. In addition, you may contact us toll-free at 866-498-9916 to obtain additional information regarding this incident.

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 employees to report any improper behavior they witness. We deeply regret this unfortunate event happened despite all of these efforts, and apologize for any inconvenience or concern this has caused.

Sincerely,

Renz Nichols
President, Certegy Check Services

:certegy

IDENTITY THEFT PREVENTION REFERENCE GUIDE

Identity theft, in its simplest form, occurs when someone obtains and misuses your personal information without your permission, and often times without any knowledge of the activity by you. It is prudent to know about identity theft and what steps you can take to minimize your risk of potential identity theft or fraud. We recommend that you remain vigilant by reviewing account statements and monitoring free credit reports for the next 24 months.

Free Fraud Alert. A fraud alert instructs creditors to watch for unusual or suspicious activity in your accounts, and provides creditors with notice to contact you separately before approving an extension of credit. To place a fraud alert, **free of charge**, contact one of the three national credit reporting agencies listed below. You do not need to contact all three agencies; rather, the agency that you contact will forward the fraud alert to the other two agencies on your behalf. An initial fraud alert stays on your credit report for 90 days.

Equifax
Office of Fraud Assistance
P.O. Box 105069
Atlanta, GA 30348
(888) 766-0008
TTY: (866) 478-0030
http://www.equifax.com

Experian
Credit Fraud Center
P.O. Box 9532
Allen, TX 75013
(888) 397-3742
TTY: (800) 735-2989
http://www.experian.com

TransUnion
Fraud Victim Assistance Department
P.O. Box 6790
Fullerton, CA 92834
(800) 680-7289
TTY: (877) 533-7803
http://www.tuc.com

Free Credit Report. Placement of a fraud alert will also entitle you to a free credit report from each of the three agencies. When you place this alert on your credit report, you will receive information about ordering one free credit report from each of the credit reporting companies. (If you elect not to place a fraud alert on your consumer credit file, you may still receive a free credit report by visiting www.annualcreditreport.com or calling toll-free (877) 322-8228.) We encourage you to obtain free reports, and to verify that all of your personal information listed on the reports is accurate.

Review Your Credit Report. Once you receive your reports, you should review them carefully for unusual credit activities, such as inquiries from companies you did not contact, accounts you did not open, and debts on your accounts that you cannot explain. You should verify the accuracy of your Social Security number, address(es), complete name and employer(s). If your credit report shows suspicious activity or unusual credit inquiries, you should immediately notify the agency that issued the report. You may also contact your local police or sheriff's office to file a report of identity theft. Be certain to obtain a copy of the police report. You may need to provide the police report to creditors in order to address any credit problems that may arise.

We recommend that you check your credit reports and review your account statements periodically. This can help you spot problems and address them quickly.

Free Credit Freeze. You may want to place a security freeze on your consumer credit file. A security freeze prohibits credit agencies from sharing your credit file with any potential creditors without your consent. Once your files are frozen, even someone who has your personal information should not be able to obtain credit in your name. The three national credit reporting agencies require that security freeze requests be made in writing and forwarded to the addresses listed below:

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013

TransUnion Security Freeze
P.O. Box 6790
Fullerton, CA 92834

Obtain Additional Information. Additional information about personal identity theft and fraud from the Federal Trade Commission ("FTC") at http://www.consumer.gov/idtheft. You may also file a complaint with the FTC at its website or by calling 1-877-ID-THEFT. Your complaint will be added to the FTC's Identify Theft Data Clearinghouse, where it will be accessible to law enforcement agencies for use in their investigations.