

**North Carolina Security Breach Reporting Form
Pursuant to the Identity Theft Protection Act of 2005**

Name of Business Owning or Licensing Information Affected by the Breach: CERTEGY CHECK SERVICES, INC.
Address: 100 SECOND AVE. SOUTH
ST. PETERSBURG FL 33701
Telephone: 904-357-1473
Fax: 904-357-1077
Email: MARIA.VIVAS@FNIS.COM

PLEASE SUBMIT FORM TO:
Consumer Protection Division
NC Attorney General's Office
9001 Mail Service Center
Raleigh, NC 27699-9001
Telephone: (919) 716-6000
Toll Free in NC: (877) 566-7226
FAX: (919) 716-6050

Date Security Breach Reporting Form submitted: JULY 4, 2007
Date the Security Breach was discovered: JUNE 27, 2007
Estimated number of affected individuals: 2.3 Million
Estimated number of NC residents affected: UNKNOWN AT THIS TIME

Name of business maintaining or possessing information that was the subject of the Security Breach, if the business that experienced the Security Breach is not the same entity as the business reporting the Security Breach (pursuant to N.C.G.S. § 75-65(b)): SAME

Describe the circumstances surrounding the Security Breach and state whether the information breached was in electronic or paper format: EMPLOYEE THEFT

Regarding electronic information breached, state whether the information breached or potentially breached was password protected or encrypted in some manner. UNKNOWN If so, please describe the security measures protecting the information: _____

Describe any measures taken to prevent a similar Security Breach from occurring in the future: SEE ATTACHED

Date affected NC residents were/will be notified: JULY 5 - JULY 12, 2007

If there has been any delay in notifying affected NC residents, describe the circumstances surrounding the delay pursuant to N.C.G.S. § 75-65(a) and (c): NONE

If the delay was pursuant to a request from law enforcement pursuant to N.C.G.S. § 75-65(c), please include the written request or the contemporaneous memorandum.

How NC residents were/will be notified? (pursuant to N.C.G.S. § 75-65(e))
Please attach copy of the notice if in written form or a copy of any scripted notice if in telephonic form.

written notice
 electronic notice (email)
 telephone notice
 substitute notice

Signature: [Signature] Date: 7/4/07
Contact Person, Title: MARIA VIVAS
Address: 601 RIVERSIDE AVE., T-2
(if different from above) JACKSONVILLE FL 32205
Telephone: _____ Fax: _____ Email: _____



OCT - 4 2007

DEPARTMENT OF INSURANCE
State of North Carolina

1204 Mail Service Center
Raleigh N.C. 27699-1204
(919) 807- 6800

Jim Long
Commissioner of Insurance

Agent Services Division
fax (919) 715- 3794

September 26, 2007

**North Carolina Department of Justice
Roy Cooper, Attorney General
9001 Mail Service Center
Raleigh, NC 27699-9001
Attn: Consumer Protection Division**

Re: Certegy Payment Recovery Services

To Whom It May Concern:

The attached letter is being provided to your office for your information. The Agent Services Division received a letter from Renz Nichols, President of Certegy Payment Recovery Services, informing us that a former employee of theirs had taken personal information about clients and had sold it to others for marketing purposes. They have taken corrective action by launching an investigation and contacting law enforcement. Additionally, they have notified the individuals that they have determined that may be affected by this situation and provided contact information and additional resources to protect their credit.

If you should have any questions, you may contact me at (919) 807-6800 x76812

Sincerely,

A handwritten signature in cursive script, appearing to read "Steve Bryant".

**Steve Bryant, ACS, AIAA
Complaint Analyst
Agent Services Division**



**FIDELITY NATIONAL
INFORMATION SERVICES**

RECEIVED ASD

77 JUL 20 AM 9:57

AGENT SERVICES

Certegy Payment Recovery Services

Post Office Box 2864
Tuscaloosa, AL 35403
Telephone: 205.750.4130
Fax: 205.750.4133
www.fidelityinfoservices.com

July 13, 2007

North Carolina Department of Insurance
Special Services Division
1204 Mail Service Center
Raleigh, NC 27688-1204

RE: Certegy Payment Recovery Services, Inc.
License #3551 and License #2038

Dear Sir or Madam:

We are writing to notify you of an unauthorized disclosure of consumer information that Certegy Check Services, Inc. ("Certegy"), the parent company of Certegy Payment Recovery Services, Inc., recently discovered. Specifically, we recently learned that a Certegy employee had 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 card data, including name, address, telephone number, account number, expiration date (for credit cards) and, in some checking account cases, transactional data and date of birth. As a result of this incident, Certegy has begun mailing written notices to individuals whose information, we believe, was among those sold to the data broker. A copy of the notice provided to individuals is enclosed for your reference.

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. This incident 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, including engaging an outside forensic investigator, and notified the U.S. Secret Service.

Certegy's internal investigation did not reveal a breach of its firewall or other system security measures. However, the U.S. Secret Service, in its investigation, was able to identify the company supplying the information to the data broker and, with further assistance from Certegy, determined that the company was owned and operated by a Certegy employee who was a senior-level database administrator. The U.S. Secret Service and Certegy together identified the individual at issue and Certegy immediately terminated the individual. Further investigation has revealed that, to avoid detection by Certegy, the technician had removed the information from Certegy's facility via physical processes rather than using electronic transmissions. The employee's removal and unlawful use of the information occurred without Certegy's knowledge and was a clear violation of company policy.

While the investigation into this incident continues, Certegy 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. Nevertheless, in addition to immediately terminating the employee, Certegy has taken a number of actions to protect consumers. These measures include:

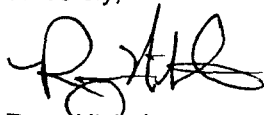
July 13, 2007

- Establishing a toll-free number that individuals can call if they have any questions, and establishing a website with additional resource material;
- Including, with the notice to individuals, a Reference Guide on how to detect, report, and protect against identity theft;
- Continuing to work closely with law enforcement officials on the investigation and a possible criminal prosecution;
- Contacting the applicable marketing companies in order to obtain the return of all consumer information;
- Initiating legal action against the marketing companies and the individual to guard against any future misuse of the consumer information;
- Contacting the three nationwide credit reporting agencies to alert them to this incident;
- Implementing a fraud watch on Certegy's internal systems for those checking accounts that were impacted; and
- 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 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 regret that this incident nevertheless occurred and, as noted, have taken prompt actions to reduce any risk to consumers.

We hope that this letter and its enclosures provide you with all the information you need. Please let us know if you have further questions.

Sincerely,



Renz Nichols
President

Enclosure

July 5, 2007

000001+000001

JOJO SMITH
123 MAIN STREET
ANYWHERE AK 99999



Reference # 70712

Important Information Regarding Account Number Ending in (9999)

Dear JOJO SMITH:

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

000001+000001

**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.

en1000-1-000001