

Q&A

Q1. What happened?

An employee of Certegy Check Services misappropriated and sold consumer information to a data broker who in turn sold a subset of that data to a limited number of legitimate direct marketing organizations. The incident does not involve any outside intrusion into, or compromise of, Certegy's technology systems.

Q2. I haven't heard of Certegy before. How did you get and what were you doing with my information?

A. Certegy provides check authorization services to U.S. retail merchants and also provides certain credit and debit card-related services to the gaming industry. Certegy maintains consumer information in connection with its check authorization business which helps merchants in determining whether to accept checks as payment at the point of sale. In addition, Certegy maintains check and credit and debit card information in connection with its gaming operations designed to assist casinos in providing funds to their customers. Certegy obtained the consumer information in question as a result of the services that it provides in connection with a previous transaction in which you either wrote a check to a retailer or obtained cash in a casino.

Q3. How do I know if my information was included in the stolen data?

Certegy is in the process of notifying consumers whose data Certegy has determined was stolen. You should receive notice within the next week if your data was included in the stolen data.

Q4: What was done with the stolen data?

A: From Certegy's investigation thus far, it appears that the data was sold to a data broker who in turn sold portions of that data to a limited number of direct marketing organizations. 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.

Q5. How do I know specifically what information about me was stolen?

At the top of your letter is a reference to the last four digits of the affected account. This account may be a banking account, a debit card number or a credit card number. If the reference is to a banking account number, the information included name, address, telephone number, bank account number and in some cases, transaction amount(s) and/or date of birth. If the reference is to a debit or credit card number, the information included name, address, telephone number, credit or debit account number and expiration date.

Q6. What if I don't recognize the account number listed at the top of my letter?

If you do not recognize the account number at the top of the letter, you will need to provide us with some additional information so that we can research what information was disclosed. We will then send you a written statement with the specific information contained in your file.

Q7. Were social security numbers stolen?

No.

Q8. What are you doing to help the affected individuals?

- Certegy has contacted the applicable marketing companies in order to obtain the return of all consumer information.
- Certegy has alerted the nation's three major credit reporting agencies, TransUnion, Equifax and Experian.
- Certegy has notified Visa, MasterCard, DiscoverCard and American Express of the incident.
- Certegy has established a procedure for financial institutions to obtain information about their customers' accounts so that they can place them on an active fraud watch.
- Certegy has implemented a fraud watch on its internal systems for those checking accounts that are implicated.

Q9. What should I do if my information was included?

Certegy recommends that you remain vigilant by reviewing account statements and monitoring free credit reports for the next 24 months. Certegy strongly recommends 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 your notification 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.

Q10. How do I get a free credit report?

On the reverse side of your notification letter is a Reference Guide giving you more information on identity theft, how to report it and how to protect yourself. That Reference Guide addresses, among other items, how to obtain a free credit report.

You can receive a free credit report by visiting www.annualcreditreport.com or calling toll-free (877) 322-8228. We encourage you to obtain free credit reports, and to verify that all of your personal information listed on the reports is accurate.

Q11. What is Certegy doing to prevent future use by the marketing companies of the stolen data?

- Certegy has filed a civil complaint 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 its future 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.

Q12. Where do I get additional information?

You can get additional information regarding this incident by visiting our website, www.certegy.com. You can also send an email to questions@certegy.com.

Additional information about personal identity theft and fraud can be obtained from the Federal Trade Commission www.consumer.gov/idtheft or by calling 1-877-ID-THEFT.

Q13. How can something like this be prevented?

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.