

Central Collection Bureau (CCB) Theft of Server – Data Security Breach Frequently Asked Questions

When were CCB's server and computers stolen?

On Friday, March 21, 2008, thieves broke into the company's offices.

When did CCB learn about the theft?

On Friday, March 21, when their offices opened.

How many servers and computers were stolen?

A total of eight (8) computers and one (1) server were stolen.

What information was accessible on the stolen computers?

The eight (8) stolen computers did not contain personal information.

What information was accessible on the stolen server?

The server contained individuals' names, contact information, Social Security numbers, dates of birth, (possibly) credit information, dates of service, and (possibly) medical diagnosis codes.

How many individuals had their information exposed?

The server contained information on approximately 700,000 individuals. However, we are not aware that the thieves tried to access the data on the sever.

Was the stolen server password protected?

Yes. The server and computers were password protected

How was the server protected?

The server was secured behind three (3) locked doors and was password protected.

Was the server encrypted?

No.

Why wasn't the server encrypted?

Encryption of laptops and servers has not been something that businesses routinely incorporated as a security safeguard. In fact, less than 50% of Indiana businesses have encrypted their electronic devices and servers. Even big technology companies such as IBM are just in the process of encrypting all of their electronic devices. Until recently, encryption was difficult to accomplish, and greatly slowed down the transmission time for the flow of information. Now, technology has improved and more companies are incorporating encryption into their devices.

Will CCB be encrypting its databases in the future?

Yes, CCB is moving towards encrypting its databases and computers.

What type of information was potentially exposed?

The stolen server contained individual's names, contact information, Social Security numbers, dates of birth, (possibly) credit information, dates of service, and (possibly) medical diagnosis codes were exposed.

What did CCB do to address this situation?

CCB promptly contacted the police and is working with the Indiana Attorney General's office. In addition, CCB promptly installed additional locks, a security system, and a motion detection system to help minimize the risk of any further unauthorized access to its information. CCB is also evaluating its overall privacy and security controls to ensure that it has adequate safeguards as new security threats become known.

Is my information safe and secure now?

Because there are so many threats to electronic information today, such as stolen laptops and other remote devices, hackers and thousands of computer viruses, no company that has personal information can ever guarantee that it is 100% safe. However, CCB took immediate action to address the security incident and is also evaluating its overall security and privacy safeguards.

What will be done to prevent this from happening in the future?

Like you, CCB wants to minimize the risk of improper access to its confidential information. The Company is taking steps to prevent this by evaluating its privacy and security overall and, as appropriate, implementing new measures.

Are there other ways in which my confidential information could be exposed?

There are many ways that data has found its way into the wrong hands from security breaches at other companies. These include lost or stolen laptops, hackers, emails sent to the wrong person, sharing passwords, improper access to computers by nosy or

angry employees, insider theft, and failing to shut off access when someone's job changes. Sometimes, these situations occur when the IT department is testing its systems and they use real information pertaining to people, rather than fictitious information, before they make sure they got it right.

What is the CCB doing to help the potentially affected individuals?

CCB alerted the three national credit reporting bureaus about this theft, so that they can apply a credit fraud alert. CCB also provided information to the affected individuals and the public through publication in major Indiana newspapers and by providing information on the CCB website about how to apply for a credit freeze, since this is the strongest form of protection against identity theft.

Is CCB offering free credit monitoring protection?

No, because now there is an even better alternative—credit freezes.

While credit monitoring lets you see if anyone has attempted to obtain credit in your name, the credit freeze law prevents them from doing this in the first place. You can sign up for a credit freeze by calling one of the three national credit reporting bureaus. Their contact information is:

Experian Security Freeze
P.O. Box 9554
Allen, Texas 75013
1-888-397-3742

Equifax Security Freeze
P.O. Box 105788
Atlanta, Georgia 30348
1-800-525-6285

TransUnion Security Freeze
P.O. Box 6790
Fullerton, California 92834-6790
1-800-680-7289

You can also obtain additional information as well as the forms for applying for a credit freeze from CCB's website at www.ccbinc.net.

Why has it taken nearly a month for CCB to announce this security breach to the people impacted?

When security breaches involve many affected individuals, many organizations, and a theft, there are lots of things to do in order to issue the notification. In this situation,

there are residents of at least 20 states affected by the security breach. It took some time to work with the police, notify the affected companies, and evaluate the requirements for notification (which vary) in each of those states.

Have you received any legal claims or lawsuits relating to this breach?

It is our Company policy not to discuss litigation or claims.

Identity Theft Information

What is identity theft?

Identity theft means that someone steals your personal information and uses it without your knowledge or consent to commit fraud or other crimes. For example, if someone opened a credit card in your name, and began buying things using that card, that would be identity theft. If they are not caught right away, the thief may build up credit by paying the first bills on time, and then when the credit card company gives him a larger credit limit, they charge more things and escape without paying for them. The credit card company thinks it is you since the card is in your name.

Is identity theft only a problem for those people whose information may have been stolen via a computer?

No. You can be a victim of identity theft in many ways. People may be able to obtain your information by stealing your credit cards, overhearing you give your credit card number on the telephone, or picking up a receipt (such as from a restaurant or gas station) that has your account on it. In addition, most companies store information about your purchase in a database. If someone accesses that database, he or she can obtain information about many people at one time.

Should I cancel my credit cards or close my bank accounts, just to be safe?

No. Unless you notice suspicious activity, such as charges you did not make, or a withdrawal that you did not make, you do not need to cancel your credit cards or close any bank accounts.

What do you mean by "suspicious activity"?

Suspicious activity could include the following:

- Inquiries from companies you haven't contacted or done business with
- Purchases or charges on your accounts that you did not make
- New accounts you didn't open

- Changes to existing accounts you didn't make (e.g., change of address, expanded credit limit, new person authorized to use your credit card, etc.)
- Bills that don't arrive as expected
- Unexpected credit cards or account statements
- Denials of credit for no apparent reason
- Calls or letters about purchases you did not make

I haven't noticed any suspicious activity on my credit cards or bank statement, but I want to do what I can to protect myself from being a victim of identity theft. What do you recommend?

If you are concerned, we recommend that you request a credit freeze from the three national credit reporting agencies so that no one can obtain credit in your name. You should also obtain a free annual credit report, and should pay close attention to your accounts.

To request a credit freeze, you need to send a letter with your name, address and some identifying information to the three credit agencies. The addresses and phone numbers are as follows: (Please note that we have included the telephone numbers in case you want to talk with these credit reporting agencies. However, they require you to send a letter to request a credit freeze. In January 2009, there will be a way to send these requests electronically, but for now, since the law was just passed, sending a letter is the only way.)

Experian Security Freeze
P.O. Box 9554
Allen, Texas 75013
1-888-397-3742

Equifax Security Freeze
P.O. Box 105788
Atlanta, Georgia 30348
1-800-525-6285

TransUnion Security Freeze
P.O. Box 6790
Fullerton, California 92834-6790
1-800-680-7289

Of course, while you have the credit freeze in place, you also will not be able to obtain new credit or a loan without lifting and then reapplying the freeze. This requires a little

extra work but will help protect you and your credit not only in this situation, but from identity theft overall.

What is the big concern about exposing my Social Security number?

These days, there is a big concern that identity thieves could use your Social Security number to pretend they are you to banks or financial institutions that offer loans or credit cards. Then, they can make charges to those credit cards or not pay back the loans, and disappear. The records will be in your name, so it will look like you did this, even though you didn't even know about it. This can affect your future ability to get credit, such as to apply for a new credit card, a car loan, or a mortgage.

What is an annual credit report?

This report will show you whether anyone has applied for credit using your information. The report is free once a year.

How do I get an annual credit report?

To order your report, you can go to the website that has been set up by the three credit reporting services for this purpose: www.annualcreditreport.com. Or, you can call them at 1-877-322-8228.

What should I do if I notice suspicious activity on my credit cards or bank account?

Act quickly. Notify the bank or financial institution at once, and discuss with them whether you should cancel that credit card or close the account. File a report with your local police station and with the police station where the activity occurred. Contact one of the three national credit bureaus to place a 90-day fraud alert on your credit report. That bureau will notify the other two bureaus to flag your file. The fraud alert flag tells creditors to follow additional procedures before opening new accounts in your name or changing existing accounts.

Equifax – 1-800-525-6285

Experian – 1-888-397-3742

TransUnion – 1-800-680-7289

You should also file a report with the Federal Trade Commission by using the FTC's Identity Theft Hotline:

- By telephone at 1-877-IDTHEFT (1-877-438-4338)
- Online at www.consumer.gov/idtheft

- By mail at Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580

Can Social Security put a flag on my number?

No. Unlike the credit bureaus, the Social Security Administration cannot put a flag or a security alert of any type on your Social Security number.

Can I get a new Social Security number?

The Social Security Administration only assigns new Social Security numbers in rare cases. You have to show that the old number has been used with criminal or harmful intent and that the misuse has caused you to be subjected to recent financial or personal hardship.

What is the US Government doing about identity theft?

The government is doing a number of things. The Federal Trade Commission has set up a system to report identity theft. They are working with state and federal officials such as the FBI, state Attorneys General, and the police to investigate and prosecute identity thieves. In addition, many states, including Indiana, have passed security breach notification laws and credit freeze laws to help people know about breaches and protect their credit. The US government is also coordinating with other countries because this is a global problem.

How many people are affected by identity theft?

Identity theft is a huge and growing problem in the US. Some surveys have estimated that one out of three Americans has been affected.

Where can I get more information about identity theft?

You can visit the FTC's identity theft website at Federal Trade Commission (FTC) website at <http://www.ftc.gov/bcp/edu/microsites/idtheft/>.