Business Credit News

CREDIT REPORTS 210-225-7106
COLLECTION 210-225-7106
E-MAIL: bcms@bcmstx.com
FAX SERVICES 210-225-1777
WEB SITE: www.bcmstx.com

Business Credit and Management Services Co of Texas
4407 Walzem Rd #205
San Antonio, TX 78218

NOVEMBER 2017

"CREDIT HACKING IS NOT NEW"

By: David Balovich

It seemed strange, when I was balancing my business account checkbook, using Chase's on-line check payment system, there were several checks I'd authorized weeks before to local businesses that had yet to clear the bank. No, apparently those payments had never reached their destinations. A quick trip to the local bank branch along with a heavy fee for stopping payment on those payments put this problem behind me.

This was not the worst of it: JP Morgan Chase was hacked in August of 2014, the computer thieves making off with, according to the *New York Times*, "huge amounts of data, including current checking and savings account information." If you remember this infamous hack, you remember that fingers immediately pointed in Russia's direction. However, if you were waiting for JP Morgan Chase to send clients a letter explaining exactly what was stolen, or whether it might affect your own accounts — my wife and I have numerous accounts with Chase and their investment bank — I hope you didn't hold your breath: Chase never sent one. Nor was any apology ever extended to those of us using their bank. Apparently, no one was concerned, especially not Chase, that alleged Russian hackers had made off with sensitive information on 83 million Chase customers' accounts. Of course, during the 2016 presidential election and even today as I write this the unconfirmed rumor that a bunch of Russian hackers influenced the American elections and immediately our "concerned about protecting its' constituents" do-nothing Congress immediately morphs into a knee-jerk witch-hunt that we had not seen the likes of since the infamous Senator from Wisconsin went looking for Communists in every American family household in the early 1950's.

But in 2014 this was considered the greatest breach of confidential financial data in the world. Then for some like me it really got personal: My accountant notified me that when he tried to transmit my tax return for the previous year, the code came up showing it had already been filed. The IRS rejected the return he tried to transmit.

That's right, someone had gotten my Social Security number and filed a false 2013 tax return to generate a cashable tax refund check. And, although whoever did this could not spell my name properly and obviously used a different address, occupation, and income, I along with several of my co-taxpayers discovered that IRS computers are not set up to flag returns even if numerous database fields are completely different from those listed on previous filed returns.

This shouldn't surprise anyone considering three years earlier in 2011, the IRS mailed 23,994 tax refunds totaling over $46 million to one, count 'em, *one* address in Atlanta. That's right, there's also nothing in the IRS computer system that will flag 23,994 refund checks going to one address as being somewhat unlikely to be legitimate. My first question, upon reading that story, was why the postal carrier or the Atlanta post office wasn't investigated by Congress or at least the General Accounting Office. One would assume that the postman or post office would question whether hundreds, or thousands, of tax refund checks going to the same location day after day might be illegal. Unless of course they were in on it.

The cost of protecting myself from this ID theft was not cheap. I had to hire a tax attorney to get the IRS to throw the phony tax return out and accept my legitimate tax filing. It was humorous if you think about it; while most Texans cry and moan about paying taxes, I'm paying an attorney to force the Treasury Department to take my money.

Now, three years later we experience the biggest hack of all, just two months ago: 143 million records out of the Equifax computers; as the media put it, "the credit files, Social Security numbers, addresses, and credit card and bank account numbers of 44 percent of the population of America." Actually, that's a foolish statistic, because kids in first grade or Pre-K probably don't have credit files — or, if they do, it's likely they haven't borrowed any money yet. So if one takes the 143 million stolen files by the number of individuals over 21 years of age, the correct percentage is that Equifax allowed the sensitive credit files of over 57 percent of all adult Americans to be stolen.

And as shocking as this story is, most do not fully understand the long-term consequences of what just transpired. Once someone has your Social Security number, name and credit score, it becomes quite easy to open new accounts in your name, or take out loans or mortgages. The first you know about it will be when you go to get new credit and you're rejected for a large past due loan you knew nothing about, much like I found out someone had stolen my identity when I tried to file a tax return. True, you can file with the credit bureau to have those illegitimate accounts removed from your file, but the media is full of stories pointing out that it often takes years to get credit files corrected.

Now consider that 90% of all businesses in this country are either sole proprietorships or general partnerships and what is one of the sources many of us business creditors use to get our information from on these individuals? (Drum roll maestro). That's right credit reports, Equifax, Experian, and Trans-Union. So much for detecting the creditworthiness of our applicants.

This is not *"breaking news"*. The Department of Justice reported in 2012, five years ago, that identify theft created financial losses of $24.7 billion in that year alone. Two years later the DOJ reported that 17.6 million Americans were victims of identity theft, or 7 percent of residents aged 16 and older. *USA Today* reported in February of this year that identity theft hit *another* 6.15 percent of all adults in 2017. And now, stated again, the Equifax hack means the financial data of 57 percent of all American adults has been stolen in one heist.

It almost takes one's breath away. But it also makes you question why Equifax bragged about its head of security in its SEC filing, not to mention paying him over $2 million in bonuses for the exceptional job he has performed. At least, right up to the point to where they realized he'd lost everyone's most sensitive data. And how does Equifax remedy this situation? They terminate their CEO and head of security and now we can sleep better knowing our credit files are secure in their computers once again,

Equifax's remedy is no remedy at all. This problem is so overwhelming that every one of the 143 million affected individuals needs to freeze their credit files immediately. If it's true that bank accounts were also stolen, they need to close and reopen new ones. At one point Equifax said only 209,000 credit card numbers were taken, but the reporting failed to say whether any cardholder or issuing bank would be notified. Or even whether that number is true or not.

I don't know about you but I have heard nothing from my bank and the emails I have received from my credit card providers have simply said their records are secure but I don't care about their records because they reported the information to the credit agencies and it was they who were hacked.

This is serious because, whether it's a new home, shopping at department stores or purchasing a new or used car, America runs on credit. And sooner or later one of these heists will be put to use and potentially devastate the financial landscape. The only thing left to see is how much of our credit information is going to be sold to criminals and/or governments, my apologies for being redundant, who intend to make the theft a reality instead of an abstract concept.

Forty years ago, in 1977 before some of you reading this were born, a salesman at a Dallas GM dealership was caught reading the obituaries and using dead people's good credit information to obtain new car loans for his customers with poor credit. The reality is that this type of crime has been going on for so long that no one really pays any attention to it, unless it happens to you, a family member, or close friend. And the hacks are so common it literally took stealing almost everyone's credit file in America to get the media to make it *"headline news"*.

Then again, it wasn't that long ago that the IRS sent 23,994 checks worth $46 million to one address in Atlanta. If that wasn't the canary screaming in the mineshaft, nothing is and how many of you remember it or aware that it occurred?

Isn't it time that we, as creditors, stop quibbling about the differences between business and consumer credit reporting (the reality is there is not much of a difference anymore) and ask our elected representatives why this has been allowed to keep happening for decades and most importantly why Congress hasn't done anything yet to fix the problem?

I wish you well.

********** **NOVEMBER 2017** **********

Day	Date	Group	Location	Time
Tues	7	Austin Construction	Saltgrass Steak House 10614 Research Blvd, Austin, TX	11:30
Tues	7	Corpus/Victoria/Laredo	Holt Cat, Corpus Christi TX	11:30
Wed	8	Rio Grande Valley	Conference Call 1-800-791-2345	2:30
Thurs	9	SW Food Credit Group	Las Palapas, 4802 Walzem Rd, San Antonio TX	11:00
Wed	16	Fuel & Lube/Heavy Eq.	Phone Conference Meeting 1-800-791-2345	2:30
Thurs	16	Austin Ad Media	Phone Conference Meeting 1-800-791-2345	2:00
Thurs	16	HVAC Credit Group	********** Cancelled Meeting **********	
Fri	17	SW Electrical Group	The Onion Creek Country Club, Austin TX	11:30
Tues	21	Austin Construction	Saltgrass Steak House, 10614 Research Blvd, Austin TX	11:30
Tues	25	SA Construction	Las Palapas, 4802 Walzem Rd, San Antonio TX	11:30

****

CREDIT REPORTS……

INDUSTRY CREDIT GROUPS…….

COLLECTION RECOVERY……..

A company with financial problems does not acquire them overnight. It has usually experienced one to three years of surfaced difficulty. The earlier these warning signals are identified and analyzed the greater the chance of effective correction action.

Are you using BCMS Credit Reports and Industry Group Meetings to help you identify and analyze? Are you using BCMS Collection Recovery for the past due account(s)? Call BCMS, for all your credit needs and service at (210) 225-7106 or 800-256-5306.

BCMS COLLECTION SERVICE

Our collections staff is willing and certainly able to take on those tough, overdue accounts to which you've been devoting too much of your valuable time. We act promptly, personally contacting the debtors on the same day we receive your accounts. We are equal opportunity collectors, that is, no matter where your debtors live in the nation or who they are, we will find them and collect. In cases where we don't collect, we charge no fee, albeit we do so grudgingly…..we don't like failure. For your protection, all funds collected are placed in trust accounts. Also, all employees and attorney's are bonded. When you hit that wall in your collection efforts, give us a call at (210)225-7106.