KrebsonSecurity
In-depth security news and investigation

Experian API Exposed Credit Scores of Most Americans

April 28, 2021 71 Comments

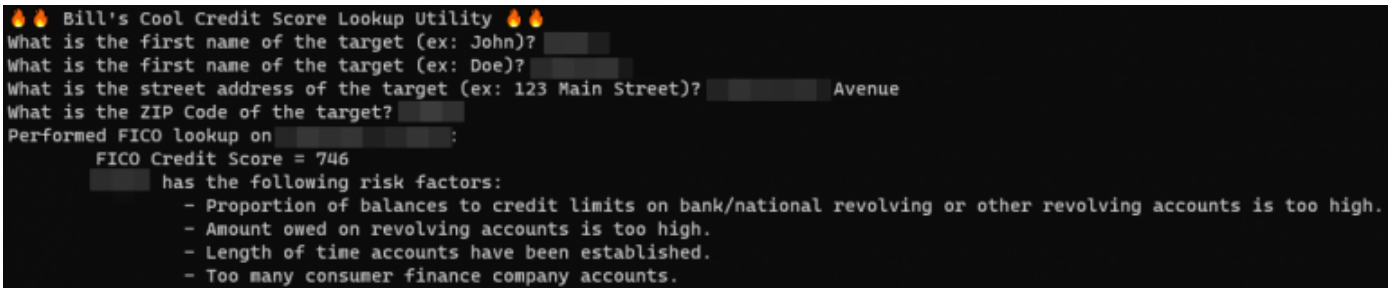
Big-three consumer credit bureau Experian just fixed a weakness with a partner website that let anyone look up the credit score of tens of millions of Americans just by supplying their name and mailing address, KrebsOnSecurity has learned. Experian says it has plugged the data leak, but the researcher who reported the finding says he fears the same weakness may be present at countless other lending websites that work with the credit bureau.

Bill Demirkapi, an independent security researcher who's currently a sophomore at the Rochester Institute of Technology, said he discovered the data exposure while shopping around for student loan vendors online.

Demirkapi encountered one lender's site that offered to check his loan eligibility by entering his name, address and date of birth. Peering at the code behind this lookup page, he was able to see it invoked an Experian Application Programming Interface or API — a capability that allows lenders to automate queries for FICO credit scores from the credit bureau.

"No one should be able to perform an Experian credit check with only publicly available information," Demirkapi said. "Experian should mandate non-public information for promotional inquiries, otherwise an attacker who found a single vulnerability in a vendor could easily abuse Experian's system."

Demirkapi found the Experian API could be accessed directly without any sort of authentication, and that entering all zeros in the "date of birth" field let him then pull a person's credit score. He even built a handy command-line tool to automate the lookups, which he dubbed "Bill's Cool Credit Score Lookup Utility."



Demirkapi's Experian credit score lookup tool.

KrebsOnSecurity put that tool to the test, asking permission from a friend to have Demirkapi look up their credit score. The friend agreed and said he would pull his score from Experian (at this point I hadn't told him that Experian was involved). The score he provided matched the score returned by Demirkapi's lookup tool.

In addition to credit scores, the Experian API returns for each consumer up to four "risk factors," indicators that might help explain why a person's score is not higher.

For example, in my friend's case Bill's tool said his mid-700s score could be better if the proportion of balances to credit limits was lower, and if he didn't owe so much on revolving credit accounts.

"Too many consumer finance company accounts," the API concluded about my friend's score.

The reason I could not test Demirkapi's findings on my own credit score is that we have a security freeze on our files at the three major consumer credit reporting bureaus, and a freeze blocks this particular API from pulling the information.

Demirkapi declined to share with Experian the name of the lender or the website where the API was exposed. He refused because he said he suspects there may be hundreds or even thousands of companies using the same API, and that many of those lenders could be similarly leaking access to Experian's consumer data.

"If we let them know about the specific endpoint, they can just ban/work with the loan vendor to block these requests on this one case, which doesn't fix the systemic problem," he explained.

Nevertheless, after being contacted by this reporter Experian figured out on its own which lender was exposing their API; Demirkapi said that vendor's site now indicates the API access has been disabled.

"We have been able to confirm a single instance of where this situation has occurred and have taken steps to alert our partner and resolve the matter," Experian said in a written statement. "While the situation did not implicate or compromise any of Experian's systems, we take this matter very seriously. Data security has always been, and always will be, our highest priority."

Demirkapi said he's disappointed that Experian did exactly what he feared they would do.

"They found one endpoint I was using and sent it into maintenance mode," he said. "But this doesn't address the systemic issue at all."

Leaky and poorly-secured APIs like the one Demirkapi found are the source of much mischief in the hands of identity thieves. Earlier this month, auto insurance giant Geico disclosed that fraudsters abused a bug in its site to steal drivers license numbers from Americans.

Geico said the data was used by thieves involved in fraudulently applying for unemployment insurance benefits. Many states now require drivers license numbers as a way of verifying an applicant's identity.

In 2013, KrebsOnSecurity broke the news about an identity theft service in the underground that programmatically pulled sensitive consumer credit data directly from a subsidiary of Experian. That service was run by a Vietnamese hacker who'd told the Experian subsidiary he was a private investigator. The U.S. Secret Service later said the ID theft service "caused more material financial harm to more Americans than any other."

Additional reading: Experian's Credit Freeze Security is Still a Joke (Apr. 27, 2021)

This entry was posted on Wednesday 28th of April 2021 04:47 PM

A LITTLE SUNSHINE

BILL DEMIRKAPI CREDIT SCORE LOOKUP TOOL EXPERIAN GEICO ROCHESTER INSTITUTE OF TECHNOLOGY

71 thoughts on “Experian API Exposed Credit Scores of Most Americans"

Rod Fuller

April 28, 2021

How long do we have to put up with Experian's incompetence? Are they not SOC certified? Which means they've checked out all their partners to make sure they aren't exposed too, right???

C Shafer

-

April 29, 2021

SOC attestations (there is no certification body for SOC reports) are only as good as the controls they implement to meet the trust services criteria. Obviously Experian's controls for application development, logical access, and vulnerability management could use a thorough review.

GMMiller

-

April 30, 2021

This is what happens when companies grow to big and powerful, overconfidence.

Catpaws

-

April 30, 2021

In 2015, millions of persons had their personal information exposed by Experian. TIme for Experian to be put out of business.

Anonymous

-

April 30, 2021

Why would you think SOC let alone the more involved SOC 2 Type II or any other compliance audit would protect against this? It's box checking. Some companies won't prioritize proper time for programming nor will they want to spend more money on audits. You can spend a few thousand bucks and it'll satisfy SOC 2. It's a complete joke. You need a record of penetration testing and no one is perfect. They miss stuff. Which is why you need multiple. They don't even need to see your code. They probably should! But they don't need to. Those certificates are 100% useless. I literally know of government servers being compromised running cryptocurrency miners on them (well they found out and fixed it, but it did happen).

We built such amazing technology. Amazing advances went into security and cryptography. The world just flushed all that work down the drain. Ignored it and now we have created the best, most exciting, world for hackers. It's like being in the 80's and 90's all over again. Everything is just there for the taking.

Ironically the best defense the world has is the fact that stolen credit cards are so abundant that they don't have much value on the black market so the odds of yours being stolen is high, but actually used fraudulently is low. That's a special messed up kind of comfort.

vanstack

-

May 1, 2021

Why would you think SOC let alone the more involved SOC 2 Type II or any other compliance audit would protect against this? It's box checking. Some companies won't prioritize proper time for programming nor will they want to spend more money on audits. You can spend a few thousand bucks and it'll satisfy SOC 2. It's a complete joke. You need a record of penetration testing and no one is perfect. They miss stuff. Which is why you need multiple. They don't even need to see your code. They probably should! But they don't need to. Those certificates are 100% useless. I literally know of government servers being compromised running cryptocurrency miners on them (well they found out and fixed it, but it did happen).

We built such amazing technology. Amazing advances went into security and cryptography. The world just flushed all that work down the drain. Ignored it and now we have created the best, most exciting, world for hackers. It's like being in the 80's and 90's all over again. Everything is just there for the taking.

Ironically the best defense the world has is the fact that stolen credit cards are so abundant that they don't have much value on the black market so the odds of yours being stolen is high, but actually used fraudulently is low. That's a special messed up kind of comfort..

Cyberweiser

April 28, 2021

Will our government ever step up and allow us to choose the right to be forgotten by these agencies?

Robert.Walter

April 28, 2021

Call me cynical but I wonder if this now public bug was intended to be a private feature.

Devon

-

May 1, 2021

Definitely seems like it was a feature. Enter your information to get your credit score and see if you can be approved. It didn't require authentication because it was a public web page where anyone could enter information to get started.

Tom Christopher

April 28, 2021

Credit ratings should be controlled and decided by the federal government, WITH ALL activities IN HOUSE, and not contracted out to vendors. A person's creditworthiness should not be in the hands of private companies that sell or misuse our data!

bobby wilson

-

April 28, 2021

Having a government-mandated potential scarlet letter that by definition marginalize the already marginalized seems… less than ideal. Not that the current system is good, but at least it's not a single point of failure that exists under color of law.

- No Body

-

April 28, 2021

Um… NO! If you are saying that the non-Accountable Federal Government is more trust worthy the somewhat accountable private companies… I disagree whole heartedly.

security vet

-

April 28, 2021

…the federal gov should never, ever own or create the score…

…have i said never?…

…never, ever…

Joy Peterson

-

April 29, 2021

You're kidding, right? We're going to let the federal government control our credit ratings! No thanks. The feds are the ones that are supposed to be regulating these idiots in the first place. Obviously they already aren't doing their jobs.

JamminJ

-

April 29, 2021

Although is it a bad idea to have the government control credit ratings…
The federal government has deregulated a lot of their oversight. This deregulation led to the financial crisis of 2008 (the great recession).

We do need to restore good regulation. Not “control”, but oversight.

JamminJ

-

April 29, 2021

Tom,
As you may have already read from other replies. Your suggestion is an bad idea of epic proportions.

Increased regulation and oversight, yes. But it is a huge overreaction to hand control of credit ratings to the government.

Government is just a body of people, just like in the private sector. Different motivations of course.

So although the free market's profit motivation is failing, big time. The government's political motivation has an equal or greater potential to do harm.

The real solution, is to use both the private sector and the public sector. Checks and balances need to be put in place (restored where they have be deregulated).

- David Walker

-

April 29, 2021

You think the Fed government would be better at this? Really? Like them or hate them, they receive data from your banks, your credit card companies, mortgage lenders etc. They don't make up data they just report it to those with a legitimate reason to pull that data. Try getting a car loan or mortgage without them. there would be no way for the lender to assess the risk of the loan or your credit worthiness without the 3 credit bureaus. The breach is bad and they need to address it quickly. But no way the Feds should be in charge of credit reporting or credit scores. Imagine how they could use your data to punish political opponents!!

- BRETT M SHORT

-

April 30, 2021

We definitely DON'T want the dam government anywhere near our credit busines!

JamminJ

-

April 30, 2021

This is what happens when private industry fails the people so badly. People start asking government to step in.
If you don't want the government… then how do you suggest we get private companies like these CRAs actually reform their crap? Take our business elsewhere? Can't do that, we are getting f'd over by companies we never chose to do business with.

- DANIEL A WILLIAMSON

-

April 30, 2021

Then they can the apply equity to everyone's credit scores. That will make it more fair right?

Robert.Walter

April 28, 2021

Call me cynical but I wonder if this now public bug was intended to be a private revenue generating feature.

Karl Koscher

April 28, 2021

Did this query generate a hard inquiry on their credit report?

- David Walker

-

April 30, 2021

no

JamminJ

-

April 30, 2021

It did not.

And it would not. The FICO Score alone isn't like the full history report.

bobby wilson

April 28, 2021

For as long as you are financially dependent on the FICO-backed credit hegemony, basically. You don't have to be literally completely financially independent to go without – considering that many people in America, including all undocumented immigrants not eligible for DACA which numbers in the millions, do not avail themselves to the system, but you more or less would need an alternative to the established system, be it crypto, or friends-and-family, or actual financial independence, in order to not rely on your FICO score in some way.

security vet

-

April 28, 2021

…you have no idea what you are talking about, partially misled by the article…

…if you get any credit, at any time, you have a credit record because all the merchants, banks, etc., that participate want to know if you'll pay back the loan and then they in turn report how well you do pay it back, job history, where you live, etc…

…so if you never get credit, sure you can not have a record, but most people need some credit at some point…

…and, as has been pointed out in the last article by countless people, they own the data, not you…

- corey

-

April 30, 2021

Haven't seen my report in at least 20 years. Don;t even care. I owe nobody, except property taxes and electric. More should live this way but to each their own. MY life is pretty is just about stress free. Bills are stressful.

Sandy Walker

April 28, 2021

Thank you for your continuing to report and share around these topics. I hope consumers, and governmental officials are paying attention to this. What can we do to push for positive action on this?

Portwood

April 28, 2021

I think the future will be a well balanced hybrid off online and offline systems. IE, some enterprise companies are now reverting to tape backup storage because basically “unhackable". The strategy makes sense from an operational standpoint, unless you're someone who has based your whole career over the last 10 years on Cloud certifications or invested all your infrastructure in it; ergo biased stance.

Joeh

-

April 30, 2021

What? Who is going back to tape? Only for backup that goes offline. NO ONE uses tape for active records. Speed is the reason and tape is too slow.

JamminJ

-

April 30, 2021

“Only for backup that goes offline"
“tape backup storage"
Yeah, “tape backup storage". That's what Portwood said.

G.Scott H.

April 28, 2021

“While the situation did not implicate or compromise any of Experian's systems, we take this matter very seriously. Data security has always been, and always will be, our highest priority."

That is an outright lie. The API is their creation to access their data on their systems. Unauthenticated access to data is near the top of the list of vulnerabilities, and it's remotely exploitable to boot. Since it is unauthenticated, they have no idea who is accessing the scores. At best they have IP addresses if they have enough logging enabled.

@Karl Koscher: This will not generate either a hard or soft inquiry on the credit report. In fact there is likely no way for an individual to know if their score was pulled no matter who pulled it.

In my opinion the credit rating system is leaking like a sieve. Unfortunately, they are not the only ones and a scary number of the insecure are financial related.

JamminJ

-

April 28, 2021

This API exploit not leak credit reports.
Only the credit score and a vague explanation about why it may be low.

An actual, full credit history report would definitely trigger an inquiry.
These credit reporting bureaus would not let an unauthenticated API access a full credit history. They want to get paid and they need to know who's making the request.

Dan

April 28, 2021

Brian,

Was that Experian's entire written statement? Did they not comment on the fundamental issue raised by Demirkapi of allowing FICO score pulls with only name and address? Dodging that

main point makes it sound like an intentional feature to be sold to their partners, who Experian will presumably continue to blame for not blocking queries that they themselves allow for a fee. Saying that “the situation did not implicate…Experian's systems" further reinforces the idea that their API is working just how they want it to.

And Experian conveniently never claimed to have done any kind of genuine investigation expected to detect other vulnerable partner websites. Clearly they didn't have effective detection/response before now. So far we don't know if they are even attempting to develop the capability to very that the other partners they trust with everyone's data are securing against this simple vulnerability.

Experian may “have been able to confirm a single instance of where this situation has occurred" without any focus on the vulnerability, but instead by searching logs. Did they know that Demirkapi's recent tests resulting in successful FICO score pulls used a DoB of 00/00/0000? Or maybe Demirkapi used his own name in initial tests on the vulnerable website.

- BrianKrebs Post author

-

April 29, 2021

Yes, sadly it was their entire statement. Nothing about how they're reviewing their processes to make sure this isn't a problem in other places. They didn't answer any of my follow-ups, including the lack of real authentication.

J. A. DeLuz

April 29, 2021

The Credit Nazi's, all four of them, need to be defanged, if not dismantled completely. They have far too much power, are too insecure, and have far too much influence on our daily lives. Some actions can ruin you for 10 years. Now, NO-ONE but a judge should be able to do that!

Will

April 29, 2021

Experian “lost" 50 million people's complete information, then immediately started selling security against that right after. According to their commercials, they want you to give them pertainent information about yourself and they'll give you an incredible boost of 8 or 10 points on your score. It takes a 700 score or better to have a great score, doesn't it? Is there a pattern here?

Ron

April 29, 2021

How hard can it be to actually authenticate a user before dishing out private information? This is just embarrassing

Zackis

April 29, 2021

Bless you Mr. Krebs for keeping up the good fight 🙂 What a crappy place we are in when protecting your credit and your identity is made rather difficult by the three agencies no one ever wanted. Keep up the good fight 🙂

Jack

April 29, 2021

As much as I'd like to jump on the bandwagon of “I don't understand how credit or lenders work and I'm ANGRY ABOUT IT" I can't. I actually understand how API's and credit scores work. It sounds like the article spin and title are misleading based on ignorance here.
Brian- you left out the word POTENTIALLY when you said it “exposed credit scores of most Americans". You should be thorough, not alarmist. There is NO REASONABLE information to suggest that this was exploited 300 million times. Poor wording and you are asserting that DID happen. That doesn't seem responsible.
The lender or financial partner was almost certainly authenticated for the API call. You could prove that wrong by bypassing the lenders and directly calling the Experian API – nobody did that here, right? I'm saying the LENDER was authenticated, just not the consumer. That level of nuance seems to be lost here.

Also, unlike your credit report details, FICO score is not really protected by the FCRA (Fair Credit Reporting Act) so “need to know/existing business relationship" is not needed the same way. Again, details lost on this article apparently.

From any credit bureau or data broker's view- an authenticated and paying customer (lender) has a request and provided partial info- if you can match it to the individual record you supply the data. There may be a contract that says that customer will properly identify and validate all consumers before sending the query, i.e. follow the law, but that is on them.

The suspicion that all lenders are not identifying their customers is just wild speculation- I am not saying it is right or wrong, it just needs to be identified as what it is- a guess based on ignorance of the whole topic of how these systems work in reality.

JamminJ

-

April 29, 2021

“The lender or financial partner was almost certainly authenticated for the API call. You could prove that wrong by bypassing the lenders and directly calling the Experian API – nobody did that here, right?"

Read the whole article… it was proved by Bill Demirkapi, an independent security researcher at the Rochester Institute of Technology
“Bill's Cool Credit Score Lookup Utility" calls the API directly.
“Demirkapi found the Experian API could be accessed directly without any sort of authentication"

—

“exposed credit scores of most Americans"
“suggest that this was exploited 300 million times"

The term “exposed" is not the same as “exploited".
Maybe it does require some critical reading and/or an understanding of cybersecurity terminology. I doubt many were mislead by the term “exposed". An unauthenticated API is a very good example of “exposure" while not suggesting “exploitation".

—

But I do agree… the FICO score is not protected information. It is a nuanced data privacy conversation that needs to be had. Some people, who also failed to grok the entire article, have assumed an entire Credit Report was exposed by the API. Nope.
I am less worried about a credit score. Honestly, I don't consider that information to be private nor owned by the individual. It's a reputation score, like number of stars on an Amazon account. It is not for the account holder to keep private, but for all potential lenders (customers) to see, so they can make a semi-informed decision about giving you money.

Jack

-

April 29, 2021

Ok, right the article claims the Experian API was directly accessed- but doesn't prove that. I initially thought they meant directly to the lender's interface (rather than filling out their web form). That isn't clear either way.
If the consumer sees the 3rd party API endpoint directly, that means the lenders code was depending on the client browser to initiate the connection to Experian (e.g. javascript) and that is not a normal pattern. Without authenticating the requester would mean Experian is giving away free service (they've failed to monetize their API and work). That is their choice I suppose but poor business practice even for a CRA.

“Exposed” is still open to interpretation I guess as it has multiple meanings. i.e. vulnerable vs. revealed. I will concede that point, but still object to omission of the word potential.

Jack

-

April 29, 2021

Also, if the connection was not via the lender then the fact that the lender has disabled this functionally is meaningless, and they could still go directly to the Experian API endpoint. That context is what I think contradicts the claim that the connection was “direct”, it implies direct to the lender org, which is now disabled.

JamminJ

-

April 29, 2021

“We have been able to confirm a single instance of where this situation has occurred and have taken steps to alert our partner and resolve the matter," Experian said in a written statement

“he suspects there may be hundreds or even thousands of companies using the same API”
“They found one endpoint I was using and sent it into maintenance mode”
—
“the fact that the lender has disabled this functionally is meaningless, and they could still go directly to the Experian API endpoint”
—
Yes, exactly the point of contention. The security researcher said this was what he feared Experian would do, merely alert the one lender which does not fix the underlying problem.

JamminJ

-

April 29, 2021

The article doesn't provide proof, no. Krebs doesn't really do that, he summarizes and reports. The security researcher will provide proof on his blog, after a period of responsible disclosure.

—

"that means the lenders code was depending on the client browser to initiate the connection to Experian (e.g. javascript) and that is not a normal pattern"

Yes. This unfortunately is a mistake that is all too common. Doing client side, what should be server side, is not good practice, but happens all the time.

—

"would mean Experian is giving away free service"

Yeah. Could be a promotional service. The FICO score is often the "free" teaser CRA's offer, in order to get customers to buy the whole credit report history.

I know of several banks that offer an instant FICO score. I don't know what CRA is being used, or whether the API is authenticated or not.

mysec

-

April 29, 2021

I agree with your point that the wording of the article could have been more specific. But shouldn't Experian be responsible for vetting their customers (lenders) to ensure the have proper security controls are in place?

If Experian wasn't responsible then why did they take action..

Jack

-

April 29, 2021

Yes, credit bureaus and data brokers in general do vet their customers. As a consultant with wide experience, I've seen entire teams dedicated to doing this. I'm aware that the CRA's (specifically) and data brokers (generally) often terminate access to their systems from both illegitimate customers and customers who have a rogue employee abusing the access. Those are often the sources of data for sale on the darkweb, for example, and it threatens their revenue so it makes sense the data provider is incented to act. However, they won't have access to their customers code.

My guess is Experian took action because they saw a customer who was not following the contractual agreement. That shouldn't be misinterpreted as responsibility for the customer actions or customer code.

Mark Weatherford

April 29, 2021

What's really ironic here is that trying to get your own credit score from Experian requires the navigation skills of Magellan and the patience of Job.

Jack

-

April 29, 2021

Not really surprising, the CRA's are all focused on automated system-to-system calls, such as from banks and lenders systems. The human interfaces and specifically the public-consumer facing user interfaces are not their focus. I bet the volume is like 100:1 so the "1" doesn't get the funding or support. That would likely be true at any business, right?
But, I certainly agree and think all three big CRA's have terrible consumer interfaces. It's like they are 10+ years behind (and were bad by 2010 standards at that). Those capabilities do not inspire confidence. 😀

random

April 29, 2021

Let me guess.
Outsourced to some cheap IT company in India to build this API and more?

Why

-

April 29, 2021

Racist much?

This is not a mistake that is blamed on poor coding. This is the business (capitalism) having a profit motive that supersedes privacy concerns.

Catwhisperer

April 29, 2021

I love it, please open an account in my name so I can increase my credit score. Checking with my bank, my credit score is … 4. Yes that is not a typo, I've been trying for years to get it to 0. Maybe Bill there can help a brother out! 😀

xcv

April 29, 2021

If your credit hacked, you lose your home to pre-emptive foreclosure just like that. The banks have clauses in the fine print allowing them to do that even if you keep up on your mortgage payments.

JamminJ

-

April 30, 2021

Citation needed.

Joe

April 30, 2021

Biden's Plan To Change Credit Reporting And Scoring

The Biden administration has a big target in its sights, or rather three big targets—Equifax, TransUnion and Experian. If President Biden has his way, he will create a public credit reporting agency (CRA) to compete with the three major credit bureaus and maybe one day replace them altogether.

https://www.forbes.com/advisor/credit-cards/president-bidens-plan-to-change-credit-reporting-and-scoring/

J

-

April 30, 2021

Thanks for the heads up about the Power Grab.
Yeah, because the IRS for example is a great case study of how awesome the federal government runs and maintains a modern computer infrastructure with tons of data. (it's a nightmare in case you didn't know).
Also the federal government is no more immune to bad code or getting hacked than private industry. Lowest bidder results anyone? I speak from personal and professional experience there.
I can hear it now… vote for the right person and get +25 points added to your credit score! Or rather… your score mysteriously drops -250 points and nobody can tell you why… but they know who you voted for or contributed to, etc. That could financially cripple you… at which point are you truly a free citizen? Better not speak out against The Party!
Anyone is lucky if they don't have to deal with the capricious bureaucrats, who don't effectively answer to anyone, at the local, state, or federal level… hope you never do.

JamminJ

-

April 30, 2021

Good. These companies have grabbed power away from the people for long enough.
They spend millions/billions of dollars lobbying Congress to deregulate and remove accountability, so they can make more profit, deploy golden parachutes, fund lavish lifestyles, cheat their rich kids into schools, and pad their own retirement.
Bureaucrats or capitalist robber barons… take your pick.
—
And remember, the Great Recession was caused, in part, due to deregulation of the private sector financial industry… particularly credit ratings of bundled derivatives. Mortgage backed securities bundled and given triple A ratings when they were full of subprime assets. There was a “pay to play” scheme going on that led to credit ratings being wildly inaccurate. Sound familiar.
—
“federal government is no more immune to bad code or getting hacked than private industry”
True. But this issue with Experian, and most of these CRA privacy issues… ARE NOT from coding mistakes or hackers. It is the result of marketing and sales people, superseding privacy and security. This are not bugs, these are features of the precious “free market” economics. It looks so nice on paper… until the reality hits, that you're not a paying customer and therefore are a product being bought, sold, and bartered away without your consent.
—
This is the 3rd time you've changed your handle, and ranted about the IRS.
Looks like you didn't get the tax refund you wanted… Get over it. Your personal grievance with the IRS has no relevancy to the topic at hand.

–

I happen to agree with the common consensus here, that the federal government SHOULD NOT “control” credit ratings. They should heavily regulate the industry under strict data privacy law. They should provide oversight.
And at most, as Biden seems to want, create a “public CRA” to compete with the big entrenched CRA's who have been failing us for so long. Credit reporting should really NOT be strictly a free market business. Nor should it be strictly socialized. It is an essential part of the economy that is often twisted and abused by for-profit companies. So the answer, as I have stated before, should be a mix. Private industry manages… under strict oversight from the federal government.

JamminJ

-

April 30, 2021

The Biden administration has a big target in its sights, or rather three big targets—Equifax, TransUnion and Experian. If President Biden has his way, he will create a public credit reporting agency (CRA) to compete with the three major credit bureaus and maybe one day replace them altogether.

Joe

April 30, 2021

Credit scores may soon be based on your web history

https://finance.yahoo.com/news/credit-score-based-history-183000645.html

Patricia A Knettle

April 30, 2021

I never signed up for experian, but they informed one of my credit cards and consequently, my credit was reduced from $1000.00 to $$250.00 I didn't appreciate experian's interference.

Jack

-

April 30, 2021

You have that backwards. Your lender requested the information from Experian, and in fact payed for it. Experian didn't push it on the lender or “interfere”. That is standard practice by banks, lenders, financial companies, etc. They both provide and request the info.
Even if you read the fine print in your agreements with lenders, it can be vague. But let's be honest- 90% of people don't read the fine print which is why they don't understand how credit reports or credit scores work.
You (the consumer) don't sign up with Experian (or Equifax or TransUnion) but the lenders do. You agreed to let the lenders share that information with “business partners and others to facilitate providing the service to you” etc. So you can get mad at the credit bureaus, but the lender wasn't going to do business with you at all without that shared history information.
So to turn it around, Experian (or other CRA's) helped the lender decide to give you the credit card in the first place- and $250 limit (based on your history of paying bills- or not) is better than $0.

JamminJ

-

April 30, 2021

Yes, very accurate. People have to understand that credit is not an entitlement. Whether you want a loan to buy a home, car, or just some upfront services like utilities or a cell phone service… Credit his people lending you money for a period of time. Those lenders have every right to know your credit history.

On the flip side, I do wish there was legislation to require simple to understand, plain english, summarized user agreements. A single page that does not need to be deciphered or translated from legalese. Long user agreements get abused by companies to confuse and ultimately get users to not read the document.

joe

-

April 30, 2021

Your credit card company reached out to them and asked for that info. Not the CRA fault and you have ways to challenge what they have on you I you think it is wrong.

Franco

May 1, 2021

How on Earth is this possible. No wonder US businesses get hacked to pieces.

Pat

May 2, 2021

I like the copy/paste error in Bill's Cool Credit Score Lookup Utility 😉
What is the first name of the target (ex: John)?
What is the first name of the target (ex: Doe)?

Subpar Typing Skills

-

May 3, 2021

Nice catch. Lord knows I've had those Homer "Doh!" Moments myself.

Charles Montgomery Burns

May 3, 2021

"Peering at the code behind this lookup page, he was able to see it invoked an Experian Application Programming Interface or API" – this means that the API code must of been client-side i.e. JavaScript. Which suggests that the API is accessed through CORS. If this is the case, which it does sound like, it indeed means that many other endpoints would be exposed.

Sounds like a very very poorly designed API, which is pretty concerning considering the sensitive data of the data being exposed. Bad Experian!

Don Pedro

May 4, 2021

The highest trees gets the most wind – remember that boys!

Jay

May 4, 2021

All of this article and the comments should go to the Consumer Financial Protection Bureau. They have the teeth to get something done about. So does Sen. Elizabeth Warren. https://www.consumerfinance.gov/ The more people who send it, the more likely the CFPB will take a look.

Robert Maylor

May 7, 2021

If you need your credit fixed urgently with 1 month I suggest you contact aceteamcredit AT gmail dot COM, He raised my score up from 540 to an excellent 800 on all 3 bureaus in 1 month. I was at first skeptical when I contacted him but I had no other place to go for help so I gave him a try and to my upmost surprise he came through. He permanently removed all the negative items I had on my credit and increased my credit score to excellent on all 3 bureaus.