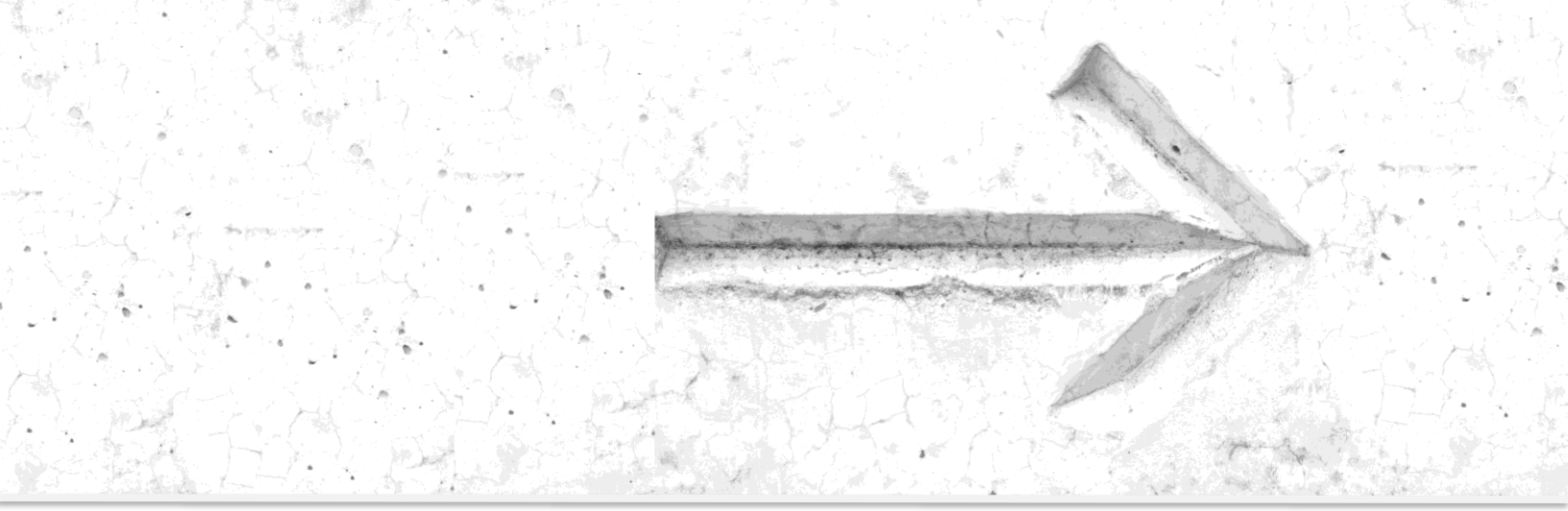

## Are you fully protected if you are just relying on credit and identity theft monitoring?

**1579**

**Breaches occurred in 2017**

Per the Identity Theft Resource Center, over 178 million points of data were stolen because of these breaches.

Are you a high net or ultra-high net worth individual? Do you think credit and identity theft monitoring is worth it? Are you currently enrolled in one of these programs? I have personally been enrolled in these programs since 2009. Does it solely give me comfort knowing that my credit and identity is protected? No, it does not. Is that surprising to you? You may be wondering why I said 'no' and why I am still signed up for it.

Knowing when credit checks are conducted, or when a card balance increases or decreases, or what my credit score is, and even being able to lock my credit are all benefits and useful information that credit monitoring products provide. Notice I said credit monitoring because identity monitoring is different. Although many of the identity monitoring solutions include credit monitoring, they are not the same. Identity monitoring includes such things as mailing address tracking, looking for new services like utilities, and cable services that have been signed up for using your personal information, social media monitoring, etc. Recently, some of the vendors added dark web monitoring to their offerings. This means you can potentially get alerts when your social security number or other personal information shows up for sale on underground sites. Those are great features, or are they?

### Credit monitoring provides information about your overall credit history.

Credit monitoring is primarily used to monitor your credit accounts, account history, and the score used by creditors to approve you for things like loans or credit cards. In certain instances, credit monitoring can prevent creditors from running a credit check on you, if the option to lock your credit is included and turned on.

Let us take a second and imagine you have a credit monitoring solution with no credit locks and your credit was run for a new credit card. You will likely get an alert telling you that a credit check was run (assuming your vendor provides it and you are set up with some type of text or app-based notification). Because the credit was not locked, it will not stop creditors from running the check and potentially opening a new account in your name. Had you locked your credit, it would have been a little more difficult for that creditor to run your credit. Now, you should know that if you are using a product from one of the three major credit bureaus, your credit will most likely only be locked with them. That means your credit could still be checked against the other two. Most creditors only require information from two of the three credit bureaus to approve applications for credit.

## Identity monitoring solutions track specific things where your personal information could be used illegally.

**16.7 million**

According to Javelin Strategy & Research, in 2017 there were 16.7 million victims of identity fraud.

Moving on to the other scenario; What if it was not you that tried to open a new credit card? What if it was someone who had access to your personal information that attempted to do it? This becomes an identity theft situation, but before we go there remember you are still dealing with someone trying to open a credit card in your name. Technically because you only have a credit monitoring solution and your credit was not locked, the creditor could still run a credit check and possibly approve the application. Again, with credit monitoring, you will likely get the alert and can quickly notify (if you are paying attention to the alerts) the creditor that it was not you that applied for the credit card. You will work with them to close the account, etc. If you also had an identity monitoring solution you may be able respond even quicker to this incident, and potentially even get someone from the identity monitoring company to assist. The biggest and probably most worthwhile benefit with identity monitoring solutions is that you can usually get someone to assist with stolen identity incidents.

Up until this point credit and identity monitoring solutions look like a no-brainer, so you may still be wondering why I said I do not take comfort in solely using them. To put it simply, these solutions just provide monitoring of select information. With certain products you get a bit more, like getting assistance from a person on stolen identity incidents. Sure, these are great to have, but do not let the creative marketing behind these solutions provide a false sense of security. The reality is credit and identity theft are very difficult to prevent, especially nowadays.

| Type of identity theft fraud | Percent |
|---|---|
| **Miscellaneous identity theft (2)** | **51.9%** |
| **Credit card fraud** | **16.8** |
| New accounts | 12.7 |
| Employment or tax-related fraud | 10.1 |
| Tax fraud | 7.5 |
| Phone or utilities fraud | 7.4 |
| Bank fraud (3) | 6.4 |
| Loan or lease fraud | 4.2 |
| Government documents or benefits fraud | 3.2 |

Some additional examples will help illustrate my point. Let us start with the solutions that offer dark web monitoring. A brief description of the dark web: It is the part of the world wide web that remains difficult to access. Finding specific things can only be done if you know where to look. There is no search engine like Google that exists. One of the main reasons people use it is to remain nameless/faceless and possibly untraceable. The dark web is oftentimes used for legitimate reasons, however, in many cases it is used for illegal purposes like the sale of your personal information, such as social security numbers, home addresses, date of birth, driver's licenses, credit card numbers, etc.

When someone advertises dark web monitoring, proceed with some caution. The dark web is called the dark web for a reason. Remember, it is already difficult to find things on the dark web, imagine trying to find 'everything'. That is an impossible task that even the best of companies have a hard time with. Many of these solutions will monitor the sites they know of but will not offer much when it comes to identifying 'new' sites where your information may exist. Your personal information can be hosted on sites where you need a special invitation to see it. It can also be shared between a very small group of people, and only those people know the site and how to gain access. Your information can show up on hundreds of new dark web sites that may only be put up for a period and then taken down, ultimately never getting detected. As you can see, there are still many challenges with dark web monitoring.

There are close to **2 billion sites** that are indexed in search engines today. However, the **deep** and **dark web** makes up almost **98%** of the sites that are **not** indexed.

Now, forget for a second what I said about dark web monitoring. Let us look at a different example. Think about a situation where your personal or credit card information could be compromised, such as from the medical documents on file at your primary care physician, or maybe the software program that stores the information on the computer systems of your attorney or accountant. Maybe a disgruntled employee at your primary care physician decided to breach your personal information to sell it to someone else, or your credit card number that you shared with a friend last year was used to make purchases that were sent to an address in a different state. Do not for a second think any of those situations are impossible. Ask yourself, who is monitoring this? What type of alert can you get for these scenarios?

There are dozens, if not hundreds of places that have your personal and credit related information. Each one of these places' handles, stores, and processes your information in different ways, some probably worse than others. If any information or data is compromised from those places the reality is bad things can start to happen from that point on. As an example, the information can be used by the bad actor who breached access to it, it can be sold in the black market by that same person, or it may end up on the dark web posted on forums or even up for sale by someone else.

The last example I want to use is one that you have probably heard about many times, Equifax. As you already know they were breached and hundreds of millions of accounts were compromised. I am certain that many of you felt victimized by it but let me let you in on a little secret, chances are your information was breached before that, maybe even more than once. It did not take the Equifax breach for your information to show up on the dark web. For those of you that have already experienced identity theft, think about how that may have happened. I'll let you in on another secret, my personal information is available on the dark web. I know for certain it was not the Equifax breach that resulted in my personal information being posted to the dark web.

So how do you prevent credit or identity theft? First, I do not like to use the word prevention because it is nearly impossible to prevent anything. I like to say, 'make harder'. You can make it more difficult for someone to want to steal your identity. Credit and identity monitoring should be two of the things you leverage to better protect yourself, but those solutions are just small pieces of the puzzle. Taking a proactive approach to identifying your risk profile (the actual risks you face) will help you better protect your credit and personal information.

**“Do not let the creative marketing fool you.”**

Here are a few things that can be done, some very basic, others require a bit more work. Some basic examples include protecting your social security card and only providing the number where it is necessary to do so (e.g. not all medical forms require you to include it). Do not willingly provide information to people who ask for it (e.g. a car dealer that wants a copy of your driver’s license to test drive a car). Avoid copying and sending documents over insecure methods (e.g. a copy of your passport to a travel agent). These are just some basic things that you can do to better protect yourself. There are many more advanced things that can be done like ensuring social media accounts are used responsibly, removing metadata from digital photos, protecting your home network, ensuring your children are not downloading applications on mobile devices that can leak personal information.

## Understand your personal risk posture to better protect yourself.

Want to find out more ways to protect yourself. Get in touch with us now and let us tell you how we can help.

## About Elteni

Elteni is a cybersecurity consulting firm offering a wide range of services to high net worth individuals, family offices, and small businesses. We are deeply experienced with technology and cybersecurity governance, risk, and compliance having worked as technologists and information security professionals and advisers, for small offices to publicly traded firms.

To learn more about Elteni, visit **www.Elteni.com**

Elteni, LLC
90 State Street
Suite 700, Office 40
Albany, NY 12207
**info@elteni.com**



Elteni