EZShield® + IdentityForce®

IDENTITY CRIME EDUCATION

The Equifax Mega Breach 1 YEAR ANNIVERSARY

Please visit our **Data Breach FAQ** to learn more about protecting your personal data.

You're Still At Risk

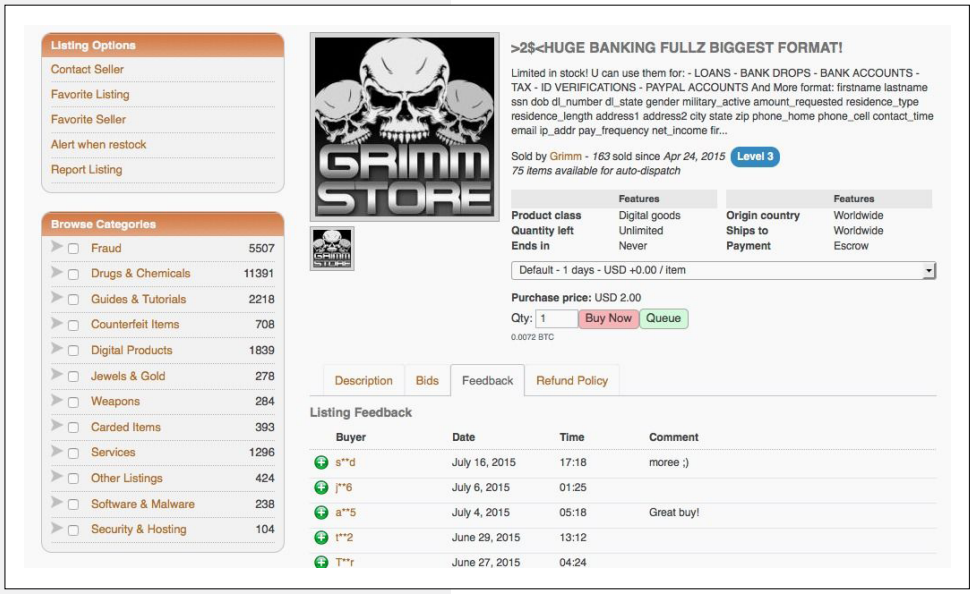
On September 7th, 2017, Equifax confirmed a data breach that affected nearly 148 million U.S. consumers. Social Security numbers, credit/debit card information and driver's licenses were among the leaked **Personally Identifiable Information** (PII), along with names, birth dates, and physical addresses.

Essentially, in the cyberworld, this breach was a Category 5 hurricane. As a result, Equifax offered all U.S. consumers free credit and Dark Web monitoring services for one year. But now, those services will start expiring between September 2018 and January 31, 2019.

Although it's a year later, the Equifax breach will continue to provide a goldmine of PII to fraudsters and cybercriminals everywhere. Once your personal information is out there – and in this case, most likely leaked onto the Dark Web – you are forever vulnerable. In fact, nearly **1 in 3 data breach victims ultimately suffer an identity crime**.[1] The exposed information won't disappear simple because some time has passed. Fraudsters often wait to misuse breached data to distance themselves from the breach and avoid being caught.

Now is the time to proactively protect your identity.

Figure 1



It's Dark Out There

To identity thieves, data breaches = profit. Breached data is often bought and sold on the **Dark Web** so that others can use it for fraud, identity theft and various other identity crimes.

According to a New York Post article from June 2018, Keeper, a password management app, claims that **hackers have stolen around $100 billion worth of personal details since 2010**. They estimate that each hacker makes around $41.47 per hour by cracking into valuable databases.

Figure 1 shows an example of the Dark Web. This is an example of one store that trades personal information records – with phone numbers, addresses, date of birth, gender, dollar amount of loan requested, and emails – all for about $2 a record. And, what's most troublesome is that the New York Post article indicated that children are 35 times more likely to have their identity stolen.

1 | Javelin Strategy & Research, 2017

2018 Tips
FOR DATA BREACH VICTIMS
WHEN YOUR PERSONAL INFORMATION IS EXPOSED

1 Beware Of Stolen Funds: It's critical when personal information is publicly exposed to continuously review your bank and financial accounts so that you can rapidly report to your financial institutions any stolen funds.

2 Monitor Your Social Media Accounts: Imposter accounts and account takeovers through any social media account can lead to fraudsters scraping personal information to even hack into email accounts, or to battle it out further on the Dark Web to buy and sell your personal information.

3 Request A Free Copy Of Your Annual Credit Report: Take great care to review your credit reports. If you find inaccurate information, contact the companies listed on the credit report(s) directly. You can also contact the Identity Theft Resource Center, a non-profit, at (888) 400-5530 to assist you, and/or subscribe to an identity and credit monitoring service to alert you when your personal information is used.

4 If You Confirm That You're A Victim Of Identity Theft, Create An Identity Theft Report With The Federal Trade Commission (FTC): Expect law enforcement to request a copy of this report when you contact them. Learn more here: www.identitytheft.gov.

5 Consider Placing An Extended Fraud Alert Or Security Freeze On Your Credit: Creditors will still have access to your credit file, even though you've placed a 7-year extended fraud alert, but must first contact you to verify your identity before extending credit. A credit freeze generally prevents creditors from accessing your credit file. To request one, you must call each credit bureau directly. Laws vary by state.

6 File Your Tax Returns As Soon As You Can: Filing an early tax return protects you from identity thieves who could file and collect your tax refund before you do. You can also request a Personal Identification Number (PIN) in order to submit a your tax return.

7 Contact The Social Security Administration: Request a copy of your wage earning report to verify that your social security number is not being used fraudulently, which could result in your owing taxes for wages earned by someone who's stolen your information.

8 Contact Your Health Insurance Carrier: Request a copy of your health insurance statement in order to identify any fraudulent medical claims.

Take Control of Protecting What Matters Most

SECURE

Data breaches only expose information, and do not necessarily mean fraud or identity theft has occurred. Focus on securing your information immediately after a data breach and be on the lookout for any new changes or activity that could be an indication of identity crime.

What You Can Do

Consider an online vault and password manager where you can store your name, address, credit/debit cards, Social Security numbers, driver's licenses and more. Additionally, identity theft protection can prove an early warning system rapidly notifying you when your personal information is at risk.

MONITOR

Especially after a data breach, it's important to know if your information has made its way to the Dark Web. Be sure that you're regularly monitoring your information and its activity whether it's through a monitoring service, or by simply reviewing credit reports and other financial statements.

What You Can Do

Our Dark Web Monitoring is a service that will continuously look for your information on numerous Online Black Market websites, chatrooms, and forums. With this service you will receive alerts any time your information has been found traded on the Dark Web.

RESTORE

If you become a victim of fraud or identity theft, restoring your identity to its original state can be overwhelming on your own. Knowing that you have a team of dedicated professionals ready to assist in restoring your identity can help to alleviate some of the stress that comes with fraud or identity theft events.

What You Can Do

We offer 24/7/365 live support and a certified Resolution Specialist so you never face identity crime alone. Our team is ready to offer 1-on-1 dedicated support to assist you in securing, monitoring and restoring your identity.

Get Proactive Identity Theft Protection

Effective ID theft protection is a combination of proactive measures, comprehensive security and monitoring tools, and restoration services. If you've opted into Equifax's free, post-breach services, you'll want to start searching for a replacement plan now. Ideally, a long-term program will provide you with a sense of security from a provider you can trust.

While you don't have control over companies and how they handle your information, you can better secure your personal information with award-winning identity theft protection services.

With **IdentityForce uniting with EZShield**, we now represent the strongest, most-reputable solutions in digital identity theft protection and cybersecurity. Ask us how our program is designed to help you address the full spectrum of identity crime threats.

About EZShield

EZShield helps trusted partners protect their most valuable asset – their customer relationships – through secure, digital identity protection and resolution services that enhance the value of existing products. The company is consistently recognized by Javelin as a **leader in Identity Protection.** Owned by the Wicks Group of Companies, L.L.C., EZShield supports thousands of **financial institutions** through its **award-winning** solutions, delivered on a secure, flexible platform that is backed by best-in-class customer support. Follow EZShield on **Twitter**, become a fan on **Facebook**, engage with us on **LinkedIn**, and join us on **Google+**. Learn more at **www.ezshield.com**.

About IdentityForce

For 40 years, IdentityForce, Inc. has provided best-in-class, highly scalable, **award-winning** identity theft, privacy and credit protection solutions to consumers, businesses, and government agencies. With IdentityForce, members benefit from the most robust and award-winning identity protection, going as deep as **Dark Web monitoring** to keep personal information safe. A pioneer of identity protection, IdentityForce's innovation and customer-centric approach has made the company a trusted partner for both organizations and individuals. IdentityForce also provides custom-tailored programs to organizations enabling them to build closer relationships and additional revenue streams. In 2015, the U.S. government awarded IdentityForce elite Tier One status as an approved provider of identity protection services for data breaches affecting over 21.5 million people. Follow IdentityForce on Twitter, become a fan on **Facebook**, engage with us on **LinkedIn**, and join us on **Google+**. Learn more at **www.identityforce.com.**