What Happens to Our Stolen Information After a Cyber Breach?
Presented by: Marla Petti

After a cyber breach, we tend to think in terms of what the victim needs to do next. Can any of the stolen data be protected after the fact? What can the victim do to secure confidential information going forward? But for a change, let's talk about the crime from the cyber thief's point of view. What does the crook do with our data once he or she has stolen it?

The going rates on the black market
First, cyber criminals use our stolen information for individual gain, opening lines of credit with our social security numbers or draining our bank accounts. They also look to make still more money by *selling* our information. In fact, there's a vast and complex underground marketplace where our stolen information is offered for sale.

The table below shows what crooks can get on the cyber black market for commonly stolen confidential data.

Type of data stolen	Average price
Social security numbers	$30 each*
Credit card information (i.e., card numbers, expiration dates, CVV codes)	$4–$8 each*
Bundles of 100 credit cards	$150**
Physical credit cards with strip or chip data	$12 each*
Health insurance credentials	$20 each*
Bank, PayPal, or other financial account credentials or numbers	Depends on the account balance

*Bankrate
**The Guardian

On their own, stolen pieces of credit card information command relatively low prices. That's because thieves can't do much damage, for example, with numbers alone; they also need to have names or billing addresses associated with the numbers. So it's no wonder that hackers look to make big scores by breaching the websites of major corporations from which they can steal thousands of pieces of information and turn a large profit by selling bundles of credit card numbers and associated data.

Prepaid cards and gift cards. Hackers also use our account information to purchase prepaid cards. They then sell the cards on the black market—in addition to actual account information—which makes for a bigger hacker payday. Other tactics include using credit card information to buy gift cards. The crooks then purchase expensive electronics or other goods with the cards and sell them at discounted prices to people who don't care where the products came from because they're getting "such a great deal."

23240 Chagrin Blvd, Suite 880 | Cleveland, OH 44122
P 216.595.6400 F 216.292.4258
hwfa.com

Bank and PayPal accounts. As for the going rates on bank account or PayPal credentials, it all depends on the bank account balance. Some hacker marketplaces sell phished PayPal credentials for a price much smaller than the account balance. The buyer purchases the stolen login ID and password from the hacker for a fee and then is free to do what he or she wants with the information.

Medical ID information. Health insurance credentials are worth even more than credit card numbers on the cyber black market because thieves can use the data to wreak greater financial damage. With stolen medical ID information, a criminal can pretend that he or she is someone else and obtain a host of expensive medical services under the real customer's name. For example, such criminals could spend beyond an actual patient's benefit limit so that, when the patient needs medical services, he or she would have to pay for those services out of pocket.

The Deep Web—where the stolen information is sold

The Deep Web is the part of the World Wide Web that is undiscoverable through basic search engines like Google or Bing. Usually only accessed through anonymous browsers and operating systems, the Deep Web masks the identity of thieves and those willing to purchase stolen information, putting these crooks completely off the radar of legal authorities. Deep Web underground markets are awash in counterfeit documents, stolen credit card data, hacker software, financial account information, and almost anything else a criminal could dream of.

Protecting yourself

Although anyone can be a victim of a major data breach—which makes it difficult for you to stop your information from getting out there—following some cyber security best practices can help keep your information secure even if it is stolen:

- **Enable multifactor authentication (MFA) on your online accounts.** With MFA, you're prompted to enter an additional piece of identifying information—typically a passcode sent to your smartphone—after you submit your username and password. That way, if your password is compromised, a hacker still won't be able to access your account without your phone and the code. (Password managers come in handy here, helping you keep all your passwords organized, so you won't have to worry about remembering them.)
- Enroll in identity protection services and keep close tabs on your credit reports.
- **Audit your medical and insurance statements regularly.** By doing so, you at least can keep tabs of any changes. If something isn't right, you can contact your health insurer and perhaps at least minimize any misuse of your information.