

## Ask the Lawyer—Identity Theft

By Sharon J. Ackah, JD, MPH  
Legal Assistance Attorney, USMA

In June 2015, the U.S. Office of Personnel Management (OPM) announced the occurrence of a cybersecurity incident which may have led to the exposure of personal information of an estimated 4.2 million current and former federal civilian employees.

Regretfully, this is not the first—and probably not the last—such incident that has threatened to unveil sensitive data for federal employees.

Therefore, knowing a few critical facts about identity theft may assist you in reducing your chances of becoming a victim, or assist you in mitigating your losses should you become a victim of identity theft.

### What is identity Theft?

Identity theft is a serious crime in which someone acquires and fraudulently or illegally uses another person's personal information, such as name, social security number, date of birth, address, account numbers or driver's license without the victim's knowledge or consent.

### What do identity thieves do with your personal information?

The Bureau of National Justice Statistics, National Crime Victimization Survey, classifies identity theft cases into three general types:

- Unauthorized use or attempted use of an existing account.

Example: The thief can empty your bank accounts, change your mailing address on your accounts and reroute things such as bank statements and checks, or simply amass debt on your existing credit cards.

- Unauthorized use, or attempted use, of personal information to open a new account.

Example: The thief can use your information to establish bank accounts; obtain credit cards accounts; establish utility or cellular service; or acquire mortgages, loans and/or lines of credit.

- Misuse of personal information for a fraudulent purpose.

Example: Using your information, identity thieves may submit false insurance claims or federal tax returns, or even impersonate you by representing themselves as you to law enforcement or medical professionals.

### What can you do to avoid becoming a victim of identity theft?

In light of the recent OPM cybersecurity incident, you should take immediate steps to review your credit reports, and pay particular

attention to your bank and credit card account statements each month to ensure there are no unauthorized transactions.

However, as a general practice, you should proactively safeguard your personal data. Take measures to protect your social security number, date of birth, bank account information and credit card numbers.

Store personal information in a safe place at home and at work. Carry your social security card in your wallet only when you need it for a particular purpose. Shred sensitive documents.

Do not respond to unsolicited requests for identifying information over the phone, through email, through social media, in the mail, or in person. Create secure and strong passwords for your online accounts and update them regularly.

### How can I tell that someone has stolen my information?

Detecting identity theft requires you to pay attention to the details! Set up monitoring systems on your bank and checking accounts, and query any unexplained withdrawals from your bank account or charges on your credit cards.

Consider electing to receive electronic statements so that your mail cannot be redirected to someone else's home. Make a list of the monthly bills you receive via email, and take notice if you stop receiving an electronic bill that you are expecting.

Acquire your credit reports from all three credit bureaus and review them carefully. Under the Fair Credit Reporting Act, each of the nationwide credit reporting companies (Equifax, Experian and TransUnion) must provide a free copy of your credit report, at your request, once every 12 months.

The three reporting agencies have set up a website, [www.annualcreditreport.com](http://www.annualcreditreport.com), to provide this free service.

### What to do if you are a victim of identity theft?

If you believe you are a victim of identity theft, you should immediately contact your bank, credit card company and other account holders to provide notice of the fraud. Second, place a fraud alert on your credit report. Third, file a police report to document the theft and allow police to investigate the crime.

Finally, send a dispute letter to the account holder of the fraudulent debt within 60 days to notify the creditor of the fraud and request that this fraudulent information not be sent to the credit reporting agencies to be included on your credit report.

## Focus on Cybersecurity

Dear West Point community,

October is Cybersecurity Awareness Month, an opportunity to focus on the practices to ensure our computer networks remain safe and secure.

The cyber threat we face today is pervasive and increasingly sophisticated. Cyber threats from near-peer nations and rogue actors will continue to plague our military, government and private sector.

Cyber attacks constantly threaten Army networks, information and personnel. It affects every one of us and can happen at any time, without warning. In the past year alone, there have been a number of high profile cyber "hacks," both in the government and private sectors, resulting in massive breaches of personal data affecting millions of people.

Unauthorized systems, such as external devices and authorized systems without proper updates, pose a threat to our network as they are not vetted. They provide a possible point of entry for malware and viruses that affect the thousands of users here at West Point by limiting access to, or altering information and can negatively impact our mission. Damage from these activities spreads and can take weeks or even months to address and resolve, often causing irreparable harm to files and folders.

The man hour and fiscal costs can be enough to render an organization's information operations ineffective for an extended period. DOD installations and universities are victims of this behavior more and more. However, simple steps with respect to access and updates can reduce the probability of an attack.

The only items authorized to connect to the USMA networks (both NIPR and DREN) are government issued devices, such as desktops, laptops and printers. The exceptions to this are Apple and Android tablets that are appropriately provisioned with AirWatch accounts. Regardless of the device, the network is for CAC-credentialed and DOD authorized users only.

There are other ways you can prevent unauthorized access to our network. Don't share your CAC card or pin with anyone else. In addition, please ensure that your device and its software are updated by leaving your system connected to the network and restarting once a day. Your systems require daily antivirus software updates.

It also should be running the latest operating system version and other client software versions in order to limit vulnerabilities. This is a continuous requirement because organizations are constantly looking for ways to infiltrate DOD and .edu systems and networks. Your Information Management Officer or Department Computer Officer can answer any questions that you may have. Social networking is an integral part of our lives and a great way to stay connected with others, but could also make you vulnerable to hacking and cyber crimes. Previously, I emphasized the importance of appropriate online behavior as it pertains to honorable living. Another aspect to appropriate and safe online behavior is keeping your personal information personal.

Check your privacy and security settings and be cautious about how much personal information you post online. The more you post, the easier it may be for a hacker or criminal to use that information to steal your identity and access your data. Additionally, you could even become a target simply based on your connection to the Army or the government.

Working together, we all play an important role in keeping our networks, information and personnel safe from harm via cyber attacks.

Beat Navy!

Superintendent Lt. Gen. Robert L. Caslen, Jr.



### How can you obtain legal assistance?

Your West Point Legal Assistance office is here to support you and provide guidance. Call us or contact us for further information. You are also encouraged to visit [www.consumer.ftc.gov/features/feature-0014-identity-theft](http://www.consumer.ftc.gov/features/feature-0014-identity-theft), which is a comprehensive website discussing

the dangers of identity theft, helpful tips to prevent identity theft and what to do if you become a victim.

Our offices are located in Bldgs. 606 and 626. The telephone number is 845-938-4541.

Find us and "Like Us" on Facebook at [www.facebook.com/USMALegalAssistance](http://www.facebook.com/USMALegalAssistance).

## POINTER VIEW

The Army civilian enterprise newspaper, the Pointer View, is an authorized publication for members of the Department of Defense. Contents of the Pointer View are not necessarily the official views of, or endorsed by, the U.S. Government, the Department of the Army or West Point.

The Pointer View © is an unofficial publication authorized by AR 360-1. The editorial content of the Pointer View is the responsibility of the West Point Public Affairs Office, Bldg. 600, West Point, New York 10996, (845) 938-2015.

The Pointer View is printed weekly by the Times Herald-Record, a private firm in no way connected with the Department of the Army, under exclusive contract with West Point. The Times Herald-Record is responsible for all commercial advertising.

Printed weekly by the

**TIMES HERALD-RECORD**

40 Mulberry Street, Middletown, NY 10940

To subscribe to the Pointer View or if you have delivery problems, call 845-346-3214.

Lt. Gen. Robert L. Caslen, Jr.  
Superintendent  
Lt. Col. Christopher G. Kasker  
Public Affairs Officer

Eric S. Bartel  
PV Managing Editor, 938-2015  
Kathy Eastwood  
PV Staff Writer, 938-3684

The appearance of advertising in this publication, including inserts or supplements, does not constitute endorsement of the products or services advertised by the U.S. Army or the Times Herald-Record.

Everything advertised in this publication shall be made available for purchase, use, or patronage without regard to race, color, religion, sex, national origin, age, marital status, physical handicap, political affiliation, or any other nonmerit factor of the purchaser, user, or patron.

A confirmed violation or rejection of this policy of equal opportunity by an advertiser will result in the refusal to print advertising from that source.

UNITED STATES MILITARY ACADEMY  
**WEST POINT**