Fighting for Their Lives

Protecting identity in the military

A naval commander's top-secret security clearance is threatened after his Social Security number is used to commit employment fraud. A U.S. Marine stationed overseas discovers $15,000 in credit card charges for purchases he never made. A military spouse is unable to buy groceries or pay rent because someone has drained the family account.

Their stories are the result of heinous identity theft crimes repeated around the world. Military personnel are prime targets for identity thieves because of long deployments and frequent relocations. Servicemembers on active duty face the greatest threat of identity theft. It can be difficult to monitor bank accounts and credit card statements while overseas. When they return home, they discover they can't get a car loan or mortgage. Bad credit can even affect security clearance and, with it, the opportunity for promotion.

Continued on page 3 ▶

Never Forget a Face

With biometrics, you are your password

It sounds like science fiction: You sit down in front of your computer's login screen, and the machine recognizes you without your having to type a word. No more keeping track of passwords or answering obscure security questions; the computer will recognize your face.

That fantasy may become reality sooner than you think. Widely used programs like Picasa, iPhoto, and even Facebook can learn and remember faces. The BioLock application for Google's Android OS will distinguish different users based on photographs. When screen shots of Microsoft's confidential plans for Windows 8 were leaked recently, it was revealed that a photo-based login is one of its planned capabilities. *Continued on page 4* ▶

Identity thieves have no compunction when it comes to stealing from service members who are fighting on the front lines, and they have no sympathy for military families left to undo the mess of compromised credit.

In this month's issue we look at the crime of identity theft affecting the military. Our story shows how service members are targeted because of long absences from home. Another factor: the overuse of Social Security numbers in everyday military life. We show what steps members of the military can take to protect themselves.

With the improvement of computer-processing power, biometrics become more likely to replace passwords and PINs as gateways to personal information. Retinal scans, voice-recognition and fingerprint technology could soon be joined by more sophisticated facial recognition technology. We look at what this means from a security and a privacy point of view.

Our Fraud Files feature Josh Becker, a young man who nearly lost a job offer when a background check turned up criminal activity on his Social Security number. An undocumented immigrant had been using his SSN for employment. Find out what happened when Identity Theft 911 fraud specialist Maria Valenzuela took his case.

Frenemy fraud rears its head again in this month's case study of a woman whose colleague accessed her personal information at the office and used it to open three credit cards, running up bills of $90,000. Identity Theft 911's fraud specialist Omar Edwards worked with her for a year to right the wrongs.

Finally, be sure to check out our Hits & Misses, a roundup of the latest fraud-related news, as well as a Q&A with Identity Theft 911's chief privacy officer Eduard Goodman, who explains what to do when your data has been compromised in a breach.

As always, we hope you will enjoy.

Matt Cullina
Chief Executive Officer,
Identity Theft 911

In this issue...

Features

Departments

Fighting for Their Lives from page 1 ▶

"Our fighting men and women all over the world are put in a vulnerable position just when our nation needs them to be at their strongest," said Adam Levin, chairman and co-founder of Identity Theft 911. "The fact that someone would disrespect our service members by stealing their identities is outrageous."

How they do it

Thieves acquire personal information by Dumpster-diving near military bases, stealing credit card numbers, or changing the address of military personnel without their knowledge.

All branches of the military are vulnerable to identity theft because of the widespread use of Social Security numbers, Levin said. Since the 1960s, Social Security numbers have been written on everything from duffel bags to dog tags.

The practice was changed in 2009, and updated identification cards only list the last four digits of a Social Security number. But if those numbers fall into the wrong hands, they can still leave a huge risk of exposure. "Only using the last four digits doesn't really provide a lot of extra protection," Levin added.

How to fight it

Experts recommend that deployed personnel place an active-duty alert on their credit report. This free service requires creditors to take steps to verify a consumer's identity before granting credit. This alert is effective for one year, and can be renewed or canceled if the deployment ends early.

"When you're on active duty you rely on friends and family to handle business for you," said Joanna Crane, manager of the Identity Theft Program at the Federal Trade Commission (FTC). "An active-duty alert eases that burden."

Deployed personnel often grant friends or family members power of attorney to manage their finances while overseas. However, this also puts military members at risk for identity fraud because it allows access to sensitive financial information.

Experts advise military personnel who are not on active duty to monitor their accounts closely, inspect credit reports, and review financial statements regularly to look for fraudulent charges. Warning signs include bills that don't arrive as expected, denials of credit for no apparent reason, or calls or letters about purchases that were never made.

Military personnel who suspect they are victims of fraud or identity theft should follow these steps:

- Close accounts that have been tampered with or established fraudulently. Follow up in writing and use the ID Theft Affidavit at www.ftc.gov/idtheft. Ask for verification that the disputed account has been closed and the fraudulent debts discharged.
- Keep copies of documents and records about the theft.
- Explain the situation to the commanding officer. A commanding officer may be contacted by creditors looking to collect charges made by the identity thief.
- File a police report with military law enforcement and the local police.
- Report the theft to the Federal Trade Commission.

The FTC has created a special military database for reporting identity theft, Crane said. The Military Sentinel is an online database that flags specific military bases that are being targeted by identity thieves. This database allows law enforcement to spot local and servicewide scams and trends, and identifies companies generating complaints from service members where they live.

"Perpetrators often hide out in companies near military bases, such as used-car dealerships," Crane said. "These are the types of places where identity thieves have been fairly successful."

Servicemembers can take steps to safeguard their personal information. The government is implementing programs to secure their data from identity predators. But it's never going to be enough until identity crimes that target military personnel are eradicated.

"Protecting our service members should be this country's top priority," Levin said. "When they are out of the country defending our freedom, it is our obligation to do everything we can to keep them out of harm's way here at home." •

How servicemembers can keep their identities safe

1. **Place an active-duty alert on your credit report. Call one of the three nationwide consumer reporting companies: Equifax, Experian, or TransUnion.**
2. **Cross-shred financial documents.**
3. **Don't give out personal information on the phone, through the mail, or over the Internet unless you know who you are dealing with.**
4. **Safeguard your military ID. Keep it with you or locked up at all times.**
5. **Never lend your credit cards or account information to anyone else.**
6. **Never click on links in unsolicited emails. Use security software to protect your computer, and keep it up-to-date.**
7. **Don't use an obvious password such as your birth date, your mother's maiden name, or the last four digits of your Social Security number.**
8. **Keep your personal information in a secure place, especially if you live in a barracks or with roommates.**
9. **Don't let mail pile up unattended. If you can't collect it, use a mail stop or post office box, or have someone you trust hold your mail while you are away.**

Never Forget a Face from page 1 ▶

So can facial recognition ever replace passwords and PINs?

"It's not far-fetched to see all these technologies come together in a few years in terms of facial recognition," said David K. Beyer, managing member of Digital Risk Resources, a pioneer in insuring businesses against online threats.

Biometrics, the measurement of a person's unique physical traits, could become a viable alternative. This is not a new idea: Other biometrics include fingerprints, retinal scans, and voice-recognition. But as technology improves, so does our ability to fine-tune these measurements, especially with facial recognition.

By then, the market may be ready. "Passwords have had a rough couple of years," added Beyer, citing a case in which a data breach led to legal action against a financial business, even though it had used the industry standard two-factor password protection.

A government report called the National Strategy for Trusted Identities in Cyberspace, prepared with the cooperation of the Department of Homeland Security, has called for new authentication strategies.

"No longer should individuals have to remember an ever-expanding and potentially insecure list of user names and passwords to log into various online services," the report stated.

"No longer should individuals have to remember an ever-expanding and potentially insecure list of user names and passwords."

— David K. Beyer, managing member of Digital Risk Resources

According to Beyer, there are two main applications of facial recognition technology: as authentication for the user, providing access to a personal machine or device; and authentication from the user, in which the user's face is scanned and compared against a database to verify his or her identity for security purposes, such as access to a building or airplane. This form of facial recognition has been used for years in military and security sectors.

States including New York and Pennsylvania have added biometric identifiers to driver's licenses in order to identify and arrest people who try to acquire multiple identities with the same photograph. These programs use proprietary algorithms to convert the unique measurements of your face—the distance between your eyes, or from eyebrow to chin—into numerical data, which can be quickly and accurately compared against vast databases of similar information.

Commercial facial recognition applications have yet to be thoroughly tested. But they're portable and highly convenient and could have distinct advantages over password and PIN-based authentication for the individual user.

In the ongoing struggle to balance user accessibility with security concerns, biometric authentication offers users a "universal password." What could be more unique, and yet more easily remembered, than your own likeness?

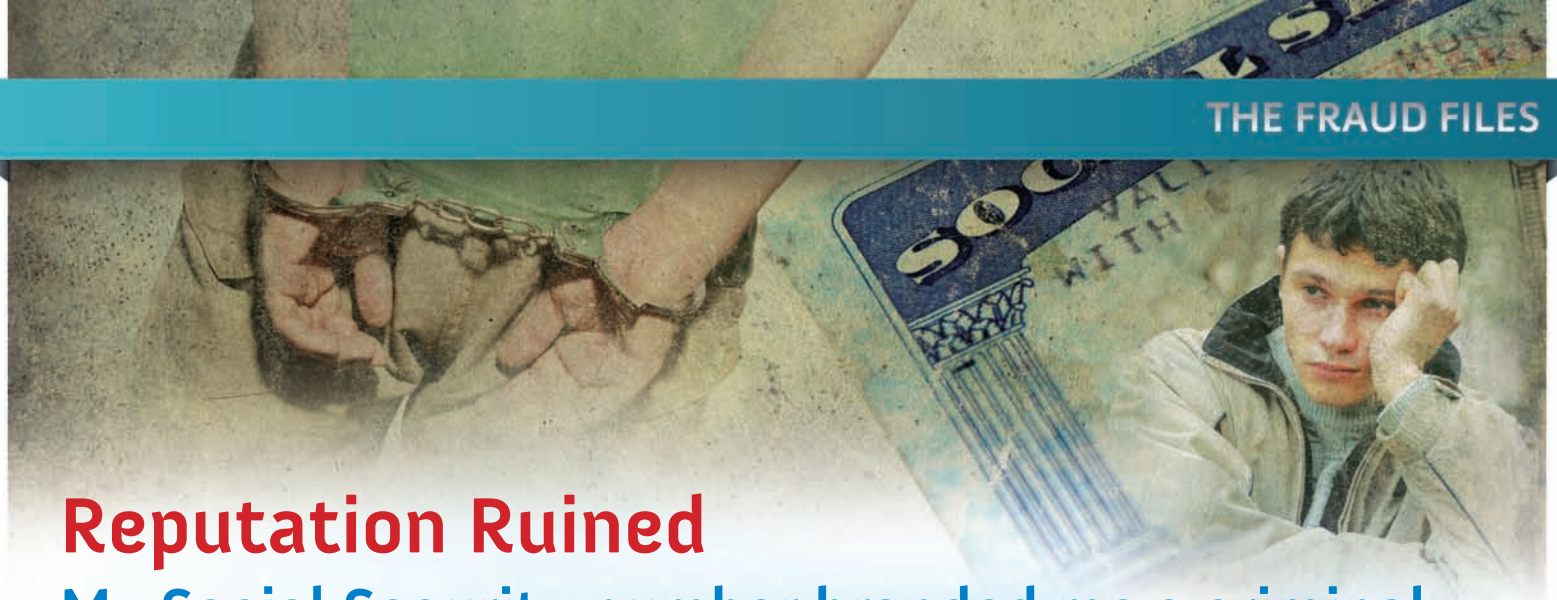
But Beyer predicts an "aha moment" once the use of facial recognition becomes widespread. "When we are no longer able to hide behind a password, we'll be more eager to protect our privacy online," he said.

After all, he says, facial recognition converts visual information into numbers, so eventually, your face is "just another data file sitting on a server," where it could be just as vulnerable as any other.

Generally, Beyer believes this new technology is not something to fear. "Facial recognition is keyed up to be what's next," he says. "But it's not a panacea."•

Get ready for biometrics

1. **Prepare for facial recognition. Do not assume that photo-scanning programs will always be opt-in. Make sure any personal photographs you store in the cloud are properly identified, and do not upload any that you would not want made publicly available.**
2. **Protect your hardware: Get in the habit of using the password protection on your smartphone or PDA so that if it were lost or stolen, no one else would have access to the camera function.**
3. **Participate in trials of new technology, and give programmers your feedback. The more information they receive, the more effective commercial facial recognition will be.**



Reputation Ruined

My Social Security number branded me a criminal

Unlike most of his college buddies, Josh Becker* wouldn't spend his summer flipping burgers or sweating it out on some construction site. He was about to land a plum first job selling electronics—one that could open countless doors after graduation.

But when a routine background check turned up "criminal activity" on his Social Security number, Becker was dumbfounded.

And suddenly, his sure thing didn't seem so sure anymore.

Security number that someone else is using it. *The New York Times* reports that each year, the Social Security Administration receives 8 million to 9 million earnings reports from the IRS filed under names that don't match the Social Security numbers.

For people like Becker, the problem comes to light only when they apply for a job or loan and get turned down.

How Becker reclaimed his good name

Desperate to hang on to the job, Becker called the service that provided his background check. No luck. They wouldn't give him information about the criminal activity.

Next, he asked his dad for help. His father turned to their insurance company, which put him in touch with Identity Theft 911.

Fraud specialist Maria Valenzuela pounced on the case. She persevered with the background-check service, reminding them of Becker's legal right to see the report since it was impacting his ability to get a job. In minutes, Valenzuela and Becker discovered that two people—himself and someone named Gloria Cortez*—were using his Social Security number. Armed with that information, Becker called the police and the Social Security Administration.

Meanwhile, Valenzuela kicked Identity Theft 911's efforts into high gear. "I called the electronics company and explained that Josh was no criminal; he was a victim of identity theft. And, thankfully, they kept the job offer open," she said.

Next, Valenzuela instructed the IRS to put a fraud marker on Becker's file. His next three tax returns will be manually audited to check for signs of fraud rather than going through the automated system.

Then, Valenzuela asked the two major credit bureaus with which Becker had a file to place a seven-year fraud alert on his accounts. That means creditors must take extra steps to verify Becker's identity before they open a bank or credit account for him.

Additional investigation confirmed that Cortez was only interested in using Becker's identity to gain employment. Though the incident still leaves him uneasy, Becker is enjoying his new job and looking forward to the opportunities that lie ahead, knowing he can count on continued support from Valenzuela and Identity Theft 911. •

Each year, the Social Security Administration receives 8 million to 9 million earnings reports from the IRS filed under names that don't match the Social Security numbers.

— The New York Times

* *Names and identifying details have been changed to protect privacy.*

When Frenemy Fraud Goes to Work

How to protect yourself at the office

Allison Keller* had a great gig. She worked with her best friend booking acts for comedy clubs in southeast Michigan.

But it was no laughing matter when Keller started getting calls from debt collectors. The punch line felt more like a sucker punch: Her friend ran up $90,000 in charges on credit cards opened in Keller's name.

Keller was a victim of frenemy fraud, when a friend or acquaintance uses your personal information to open credit cards, rent apartments, or set up new accounts—and skips out on paying the bill. Identity theft strikes 11 million people a year, according to Javelin Strategy & Research. But the crime can be doubly hard to take when the victim knows the perpetrator.

"You just have to divorce yourself from the emotional betrayal," Keller said, "and focus on what you need to do to restore your credit."

Keller's insurance company put her in touch with Identity Theft 911. With help from fraud specialist Omar Edwards, she spent the next year doing the hard work necessary to stop the fraud, prosecute the fraudster and put her financial life back in order. It wasn't easy.

They found that the friend had accessed Keller's Social Security number through their small company's employee information database. Then she used that information to open three credit cards in Keller's name—listing herself as a secondary user. She set up the accounts by using a fictional maiden name for Keller's mother, and made sure all correspondence went to her own address. She also fraudulently withdrew money for personal expenses from a company checking account to which both women had access.

"You just have to divorce yourself from the emotional betrayal and focus on what you need to do to restore your credit."

— Allison Keller, frenemy fraud victim

"Her experience is a good reminder to maintain proper business etiquette with your peers—even when you're working with friends," Edwards said. "Also be sure to follow company procedures for securing personal data."

Keller, a nonpracticing lawyer, understood better than most the steps she needed to take to deal with the fraud. She made sure the credit card companies understood she was not responsible for the charges. She registered with credit monitoring services to watch for strange activity on her credit report. She kept in close contact with police on criminal proceedings. And she and Edwards stayed in touch regularly—with Edwards making sure she hadn't missed any important steps in the fraud resolution process.

After criminal charges were filed, the woman agreed to restitution for Keller and for the credit card companies.

"I call it the lost year," she says. "It was a year of full-time work to restore my credit." For the victim, one lesson stands out: "Trust no one with your Social Security number," she says. "Guard it with your life." •

* *Name changed to protect the victim's privacy.*

Hits

What's the Frequency, Walmart?

Purdue University researcher Eugene Spafford has raised early concerns over retailers' plans to use radio-frequency identification (RFID) tags to track customer purchases. Spafford, who advises the Pentagon and White House on cybercrime, took the side of privacy advocates who reacted with alarm to retailers' plans to use RFID tracking on menswear. He told The Associated Press that a relatively inexpensive device could be used to read tags from hundreds of feet away. That information could be used to track movements within stores or to discern what products are kept in consumers' homes.

Biometric Face-off in Alaska

Sen. Bill Wielechowski, an Alaska Democrat, introduced a bill to restrict the use of biometric technology. The measure would outlaw the use of biometric data without informed and written consent from an affected individual. The Security Industry Association said the cure for potential data abuses would be worse than the hazards and would "ultimately result in the use of less secure identity solutions." According to security blog Dark Reading, the law would impose penalties that include fines of as much as $100,000 if a data collector retained or analyzed biometric data, or disclosed or distributed it to another person.

UC Berkeley Reassesses DNA Test Approach

The University of California at Berkeley revised plans for its "Bring Your Genes to Cal" program that could have left voluntary participants' genetic information vulnerable to possible mishandling. Scientists at the university had devised a program that would have allowed freshmen and transfer students to learn about three of their own genetic traits, but a state Public Health Department ruling on handling of DNA samples prompted a rollback of the program. The *Los Angeles Times* reported that the results of the approximately 1,000 participants would be made available and discussed at orientation seminars.

Misses

Patient Files Dumped in Landfill

Four Massachusetts hospitals are scrambling to tighten their records disposal policies after patient records from 2009 were discovered in a landfill. The records were found by a *Boston Globe* photographer. Some contained Social Security numbers and sensitive medical diagnoses, as well as pathology reports with patients' names, addresses, and results of breast, bone, and skin cancer tests, and of lab work following miscarriages. The inadequate disposal, which could result in fines, left Dr. Kevin Dole of Caritas Carney Hospital "absolutely shocked," he said. "We're very concerned here about protecting patient data."

Texas Restaurant Chain Hacked

A data breach at an Austin restaurant chain put an unwelcome spotlight back on Heartland Payment Systems, which last year suffered the largest ever data breach involving payment card data. The *Austin American-Statesman* said the "accounting network" at Tino's Greek Cafe was breached by hackers "somewhere between Tino's point of sale and their credit card clearinghouse company," Heartland, resulting in fraudulent charges to some customers' credit cards. The New Jersey-based company's CIO Steven Elefant told *Computerworld* that "the Heartland system at large and its merchants would not be compromised in any way by this type of attack."

British Police Create Secret Database

North Yorkshire police have been criticized for creating a secret data bank of detailed information on people involved with crimes and lodging complaints. The *Daily Mail* reported that the police district in northern England had logged data on 181,917 innocent informants, 38,259 suspects, and 107,566 victims, including their ethnicities and birth dates. Privacy advocates cited concerns about the possible misuse of the data. Guy Hosein of Privacy International said the data compilation would erode trust between the police and the public.

Q&A: Feeling compromised?

Stay alert to protect personal data

We asked our chief privacy officer, Eduard Goodman—an attorney and expert on international privacy and data-protection law—what to do if a data-breach notification lands in your mailbox. His short answer: Don't panic. Just pay attention.

My bank just sent me a notice saying my personal data may have been compromised. Now what?

Whether the trouble starts with a pilfered laptop or an insidious cyberattack, a breach of personal electronic data triggers mandatory notification laws in 46 states* as well as Washington D.C., Puerto Rico, and the U.S. Virgin Islands. If you haven't received such a notice already, chances are you will. Since the first of the year, the nonprofit Identity Theft Resource Center has tracked 449 incidents exposing more than 13 million records nationwide.

Don't panic? Doesn't this mean I'm now an identity theft victim?

Not necessarily. It means something's happened that could put you at risk. We don't have good statistics on how many breaches actually turn into fraud, because it's difficult to pinpoint when, how, and where information might have been compromised. Thieves can "bank" stolen data for years before using it.

Faced with a breach notice, most people do one of two things—both wrong. They ignore it and throw it away, or they freak out and start closing accounts. Do this instead:

1. Read the notice carefully to learn what information may have been exposed and how. (Keep the notice in case you ever need to prove that your data was compromised through no fault of your own.)
2. If you're offered a year of free credit monitoring, take it.
3. Pay extra attention to your account and billing statements. Check for charges that aren't yours.
4. After about 30 days (long enough for fraudulent activity to show up), log on to annualcreditreport.com to get a free copy of your credit report from each of the three major credit bureaus. Look for any unusual activity.

Are some breaches worse than others?

Intent is key. In many cases, a thief who breaks into a car to steal a laptop just wants to make a quick buck by selling the laptop. On the other hand, hacking incidents show real intent to profit off personal data.

The kind of information matters, too. If it's debit or credit card numbers only, there's a good chance someone will try to use them. On the upside, exposure is limited and, if your bank thinks the risk is high, it will automatically reissue new cards (effectively shutting down the identity thief).

Degree of risk gets stickier when data like Social Security numbers, birth dates, and addresses are stolen. This information has a long shelf life and can be traded internationally among organized criminals. It's valuable because, unlike a single credit card number, it can spawn dozens of new accounts. While it's less likely to be used than a single stolen credit card number (which requires much less time and work), potential damage to your good name is greater.

What should I do going forward?

Keep up your good data-management habits—cross-shred sensitive documents before throwing them away, use a locking mailbox, and take advantage of the Do Not Call and Do Not Mail/Email registries. Review your free credit reports every year. And, if you do spot something amiss, call your insurance company or bank to see if you qualify for Identity Theft 911 services. We'll help you assess your risk and, if warranted, take steps to make you less vulnerable. •

** Currently, Alabama, Kentucky, New Mexico, and South Dakota do not require businesses to notify customers of data breaches.*