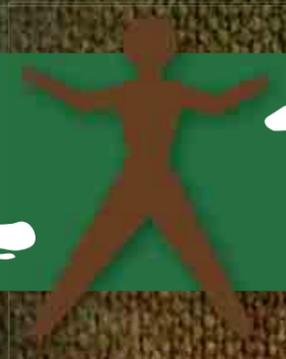


stealing

your

Reality



How thieves strip you of your identity, your cash and your sense of security

Stop the Bleeding page 38

Be Smarter page 44

Take It From Me page 48



Stop

the

Bleeding

Law enforcement's role in battling the destruction caused by identity theft

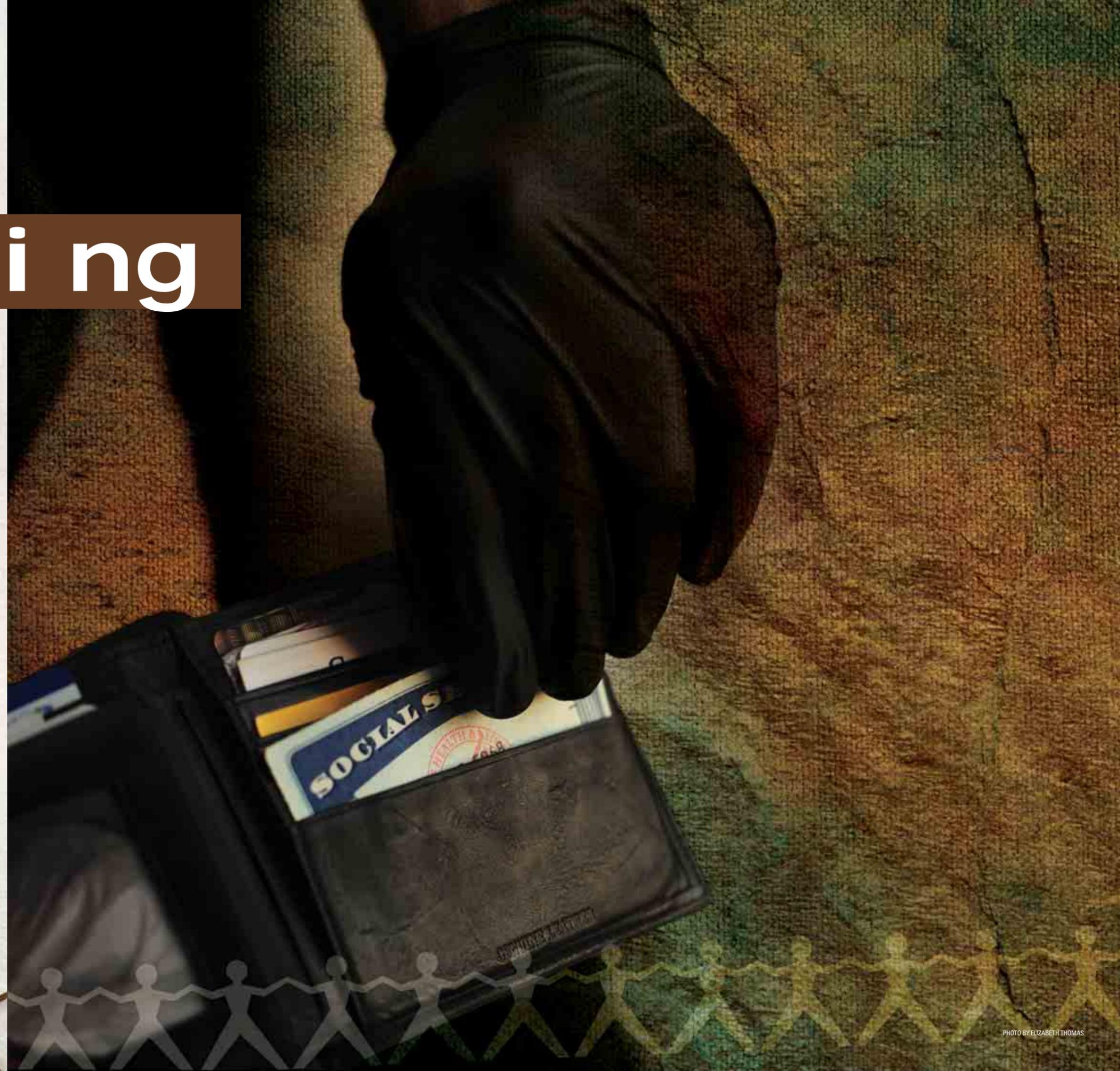
ABBIE DARST | PROGRAM COORDINATOR

Staggering debt, disillusioned security and depleted funds are only the tip of the iceberg for victims of identity theft. Identity theft is a crime that cripples its victims, not just financially, but also emotionally and mentally, as they struggle to put the pieces of their real selves back together.

Identity theft is the fastest growing crime in America with more than nine million victims each year, costing consumers billions of dollars — and never-ending grief. In Kentucky law, identity theft occurs when someone knowingly uses the identifying information of another person with the intent to represent that person for the purpose of depriving the individual of property or benefits or making some sort of financial gain, or to avoid detection. This can include using a person's name, address, telephone number, email address, social security number, driver's license number, birth date and more. And, the ways that identity thieves access this information are endless and constantly evolving.

"The notion of identity theft as someone stealing a social security number and starting an account is a very, very small piece of the whole picture — it's pretty complicated," said Hopkinsville Police Detective Burt Finley, who is one of six department detectives and specializes in computer crimes.

Identity theft to avoid detection is usually considered criminal identity theft. Criminal identity theft occurs when an imposter provides law enforcement another person's name and personal information during an investigation or upon arrest — either through a false driver's license or >>



>> identification card provided to the officer or by verbally providing the information to the officer. In many criminal identity theft cases, the imposter is cited for a traffic violation and signs the citation and promises to appear in court. If the person does not appear in court, a bench warrant may be issued, but the warrant for arrest will be under the victim's name, not the actual perpetrator. If the victim then is detained during a routine traffic stop, he or she can be arrested and taken to jail because of the outstanding bench warrant.

In other cases, the imposter will appear in court and plead guilty without the victim being aware of the event, in turn establishing a criminal record for those actions, which is now in the victim's name. Once the arrest or court information is recorded and forwarded to the national crime index database, the victim may be denied employment or terminated from employment because of a tainted background check.

The burden of clearing one's name within the criminal justice system falls primarily on the victim, who must act quickly to minimize the damage. But the responsibility to correct the erroneous data in the various criminal justice computer systems lies with the officials working within the criminal justice system. Unfortunately, there are no clearly established procedures for clearing one's

“*If the victim is detained during a routine traffic stop, he or she can be arrested.*”

wrongful criminal record, according to the Identity Theft Resource Center, or ITRC.

DAMAGING REPERCUSSIONS

However, financial identity theft is the most widely known form of identity theft. Often victims stumble across the violation in attempts to obtain funding for large purchases such as a new home or car, or even student loans. Immediately, the excitement of these new endeavors is zapped as their credit application is denied and they slowly uncover that falsely-opened accounts and surmounting debt has ransacked their credit.

Identity theft is a dual crime — it is fraud against the financial institution and it is theft of the individual's identity. If

officers do not communicate effectively with a victim and leave that person feeling law enforcement is part of the problem, officers are doing themselves and their department a disservice.

For law enforcement, knowing how to assist victims is imperative. The very first steps officers should take are to procure an initial police report or incident report and encourage the individual to immediately contact the three credit-reporting agencies and put a fraud alert on his or her credit bureau report.

“It is so important for police departments to be sensitive that [victims] need something in writing from a police officer indicating that a report has been made,” said Lori Farris, manager of the Mediation and Senior Protection Branch under the Kentucky Attorney General's Office of Consumer Protection. “It allows them to work through the creditors and produce that needed documentation. It is something [victims] have to have in hand to start piecing their lives back together and get the creditors off their back.”

Oftentimes, Farris said victims will hit a brick wall even at the initial step of going to their local law enforcement agency to file a report, because small Kentucky agencies often do not have the time, personnel or resources to work identity theft cases.

The Attorney General's Office serves as a clearinghouse to get people the information they need to help themselves. Individuals like Farris counsel identity theft victims who are angry, and tired of fighting a losing battle on their own. Even nationally, the ITRC identifies that the most frequent complaints encountered

are from victims who feel as though law enforcement just doesn't care about their plight in these particular cases. The victims believe either the officer does not consider identity theft important enough to spend time on or doesn't believe the consumer is really a victim.

Those beliefs are just a by-product of the many challenges facing law enforcement in investigating these cases. When it comes to identity theft investigations, it is not that law enforcement officers don't care about the victim's plight, but a true lack of manpower, overload of cases, lack of resources and lack of identity theft-specific training all can prohibit many agencies from offering these victims the support they desperately crave.

For victims of identity theft, no matter how big or small the loss, once the crime has been discovered, they are scared and desperate for quick answers.

“Your identity being stolen is like you've been violated — it's almost like being robbed or assaulted,” Farris said. “People are going through your personal things, so it almost feels like a physical assault.”

Since identity theft can be a repetitive crime, some victims may display symptoms associated with repeated physical assault. It feels like it will never end, especially when they keep receiving more notices by phone or in the mail from creditors, the ITRC notes. Many victims report that the financial, emotional and criminal assault on their good name takes years to recover from and has permanently impacted their lives.

WHERE TO BEGIN

That's why knowing how to work these cases and where to begin unraveling the crime is crucial for detectives today. Effective communication between law enforcement and the victim can be the difference between secondary wounding or a cooperative victim who helps the case go forward.

“When someone realizes they are a victim of identity theft, we need to stop the bleeding as quickly as possible,” Farris said.

Hopkinsville Detective Scott Raup agrees.

“The quicker the victim knows about it, the quicker we find out about it and the easier it is for us to follow up on leads,” he said. >>

File It: NCIC Identity Theft File

For years, law enforcement officers have been able to enter data on stolen vehicles, firearms and property into the National Crime Information Center files. For officers, these files are invaluable in recovering stolen property. But in 2005, the NCIC Identity Theft File was created as a means to flag stolen identities and help officers recognize imposters when they encounter them in various situations.

When victims learn they have had their identity stolen and they file a police report, the local law enforcement agency taking the report can use the victim's information to create a victim profile for the Identity Theft File, such as name, date of birth and social security number, to name a few. The victim then selects a password that can easily be recalled and is stored with the victim profile.

Since the NCIC file is available to law enforcement nationwide, when an officer encounters an individual during a routine traffic stop, for instance, a query into the NCIC system automatically searches the Identity Theft File as well. If the query matches information of an identity theft victim, the officer will receive the victim profile and the password. If the individual they have stopped does not know the password when asked, the officer may have the imposter, and not the victim.

“It is not an opportunity to arrest, but an opportunity to investigate further,” said Detective John Mellen with the Louisville Police Department's Financial Crimes Unit.

Having the information available can help tremendously in piecing together identity theft investigations that can often span several states and become difficult and convoluted.

There are a couple of conditions that must be met in order to have a profile entered in the FBI's Identity Theft File. First, each request must be supported by an official complaint record by a law enforcement agency. Secondly, documentation for the identity theft complaint must meet the following criteria before an entry can be made into the Identity Theft File:

1. Someone is using a means of identification belonging to the victim.
2. The identity of the victim is being used without the victim's permission.
3. The victim's identity is being used or intended to be used to commit an unlawful activity.
4. The victim must sign a waiver prior to the information being entered into the Identity Theft File. □



>> John Mellen, a detective in the Louisville Metro Police Department's Financial Crimes Unit, immediately contacts the victim to begin his identity theft investigation. Though the initial incident report has already been taken on the identity theft before the case is assigned to Detective Mellen, he contacts the victim to get as much pertinent information from the individual about the thefts as possible, including how they found out about the identity theft, he said.

The ITRC recommends that law enforcement agencies develop an identity theft victim guide that outlines the steps victims should take to prepare for the investigator's phone call or visit. The guide, given to victims when the initial incident report is filed, will help them organize their thoughts in order to speak clearly and concisely about the incident. It also gives victims the opportunity to get started immediately, fulfilling an emotional need for them, as well.

In that initial correspondence, Mellen said he encourages victims to keep a detailed account of every step of the investigation.

"What I generally tell people is ... to keep the report number handy and create a file for themselves," he said. "With that file they'll keep a notebook and write down every correspondence they have with anybody, to include this one — starting right today with me speaking to them — with a date and time stamp."

Once all the information is collected from the victim, the claim is then thoroughly researched. Sometimes cases can be rather simple if the victim knows or has an idea who the suspect is.

"Sometimes they'll know and say, 'My sister stole my identity and put her cable or [electric] bill in my name and she lives at this address,' so you subpoena the records from [those companies] and research the suspect and ... go out there and actually find them," Mellen said.

Between 70 and 80 percent of all identity theft cases are someone close to the victim, Mellen said. But the remaining 20 to 30 percent, where the perpetrator is a complete stranger, are much more difficult to work.

"It's finding that person initially that's the tough part," Mellen said. "With those it's just more in depth because you have to

go back, and you really have to rely on the victim to give you the records you need, like the credit report."

"The big thing is we have to know where it originated from," Raup said. "The first thing we need to know is how was this account set up — 90 percent of the time it was done online."

Once it is determined how the individual was victimized, records can be subpoenaed. For example, if a credit card was fraudulently set up in the victim's name, then subpoenaed records from the credit card company may help trace the original Internet Protocol or IP address from which the credit card was applied. Then records from that Internet provider may provide a lead to a specific address or user that may be the suspect — but it is not always that simple.

"Nine times out of 10 it's not local," Raup said. "Most of the time when we resolve one back like that, it's from somewhere else and we usually cannot figure out how and when they got [the individual's information]. More than likely they didn't even get it, but bought it from someone else."

Stealing identities for the purpose of selling them online to others for creating fake identities has become a business in today's high-tech, information-privileged society.

"If someone wants, they can pay a small fee and can pull up anything they

want on people through public records," Hopkinsville's Finley said. "There's definitely enough information available out there to steal an identity."

"The biggest distributors of false or pharmed information for use in identity theft are off shore, out of the country — and we can't touch them," he continued. "What we advise at that point is mostly damage control."

FOLLOWING THE PAPER TRAIL

Since there are so many methods identity thieves can use to steal an identity and the places they find that information are just as numerous, it is vital that law enforcement officers be aware of what kind of evidence is out there to help them investigate their cases. In financial identity theft, items such as application forms, signature cards from a checking account, records of calls made from a specific telephone number, shipping records, videotapes from security monitoring systems and bankruptcy records could hold critical evidence to help solve the case as quickly as possible. For example, the checking account withdrawal signature can provide proof that the signature on the form is not that of the victim. Also, these records can show trends, provide names and addresses where merchandise was shipped, provide potential witnesses and help pinpoint the possible location of the imposter.

“Stealing identities for the purpose of selling them online has become a business.”

In criminal identity theft, arrest, passport and Department of Motor Vehicle records may hold valuable evidence. The photo records can prove the true identity of the imposter and show conclusively that it is not the victim. These records also may point to information that establishes how the original information was obtained.

"A lot of times you'll just trip across it by doing good detective work, doing the leg work and someone will say, 'Oh, I used to work with him,' and then there you go — there's your big quote that will hone you in," Mellen said.

But investigators should also remember that they are not the only ones doing research. According to the ITRC, victims typically uncover more evidence in a case than law enforcement and do so more rapidly. Victims have an overwhelming need to be actively involved because it is their reputation and their credit at risk, and their family that will suffer if the ordeal is not cleared quickly. The center recommends that investigators teach victims how to work with them

effectively and communicate effectually with victims.

"Consumers are confused because they cannot get the information they need from law enforcement, so it is important for law enforcement to explain any reason they can't give them that," Farris said about her experiences dealing with identity theft victims. "It is also important for them to explain the process of prosecution or pressing charges."

In order to establish a solid, trusting, effective relationship between the investigator and the victim and to keep the case as straight as possible, Mellen suggests that only one detective handle each identity theft case.

"I think the key to these cases is one person handling them from start to finish, especially when the victim and the suspect are using the same name and you actually identify the suspect," he said. "These cases become so comingled, it really can get messy trying to figure out where the real meets the fake." J

Abbie Darst can be reached at abbie.darst@ky.gov or (859) 622-6453.

The Quick Three

As a quick reference guide to effectively working identity theft cases, officers should:

1. Take a report and classify it under their jurisdiction's identity theft or fraud code.
2. Advise the victim to call the toll-free fraud number of any of the three major credit bureaus to place a fraud alert on their account.
3. Encourage the victim to file a complaint with the Federal Trade Commission using the online complaint form or calling the hotline at 1 (877) ID-THEFT.

The three major credit bureaus are:

Equifax

P.O. Box 740241 / Atlanta, GA 30374
1 (800) 525-6285 / www.equifax.com

Experian

P.O. Box 9554 / Allen, TX 75013
1 (888) 397-3741 / www.experian.com

TransUnion Corp

P.O. Box 6790 / Fullerton, CA 92834
1 (800) 680-7289 / www.transunion.com

be

smarter

Staying one step ahead of potential identity thieves crouching at your door

ABBIE DARST | PROGRAM COORDINATOR

To an identity thief, you are just another number to steal. An officer's badge and training are not deterrents in this crime. It may be easier for law enforcement officers across the commonwealth to assume their position, training and experience shelters them from being vulnerable to those lurking, ready to strip them of their identity, ruin their credit and destroy their security — but it's not smart.

Identity theft is one of the fastest growing crimes in America, catching millions of people off guard every year. Law enforcement officers are not necessarily immune, and can also find themselves picking up the pieces of their identity if they are not careful and aware of the plethora of tactics and schemes identity thieves employ.

"Offenders today are doing detective work — they do what the investigators do," said Jim McKinney, instructor at the Department of Criminal Justice Training.

Identity thieves have found the ins and outs of searching for, and obtaining, people's personal data to harvest for their own deceptive use. Though the methods of identity theft are almost innumerable, there are specific types of theft ploys of which you should be aware.

GO PHISH

Legitimate-looking emails and copycat websites from financial institutions or government agencies are the basis of phishing scams. Thieves will set up false emails and website fronts that mimic businesses and agencies that individuals would trust. They send out these emails that ask for sensitive, personal information such as social

security numbers, passwords and account numbers. Oftentimes, these inquiries will even fall under the guise of keeping you safe by explaining about so-called security breaches and the need to verify information. Sometimes, the email will have a link that redirects you to a website where the information is to be entered. In a society where so much of people's correspondence is through electronic means, whether it be receiving weekly newsletters, monthly statements or frequent advertisements through email, these scams begin to look less and less fishy and throw up fewer red flags for consumers.

"Verifying information means you put in information, and they are complete scams," said Detective Burt Finley, who serves the Hopkinsville Police Department as a computer crimes investigator. "Things that can tip you off are that they ask for account numbers instead of asking to verify account numbers they provide, and there [are] just one or two places that there are slight grammar errors. Crap like that doesn't slide through on a professional site."

Simply being aware of phishing scams can help individuals make smarter choices about how they approach official-looking emails they receive. It's important to remember that legitimate companies and organizations will never ask you to verify sensitive information by email.

"If you do get these, don't enter any information," Finley said. "Never click a link. Click out and go directly to your actual site and log on directly. If there is something in there [you] need to know, it will be there for [you] in the messages section or somewhere."

Phishing scams have evolved into smishing and vishing scams, too. Smishing, like phishing, asks for confidential account information, but uses text messages sent to your phone. Vishing, or voice phishing, are automated voice messages directing individuals to call their bank or credit card company under the pretext of clearing up a problem, like theft. A number is given to call back where they then prompt for personal account information verification.

Vishing scams can seem more legitimate because people are becoming more aware of phishing scams involving email and think that if their bank was calling them to verify information, that would be a reasonable way to obtain such verifications. One way to avoid these scams is to keep a list of the numbers to personal banks and credit companies that you can call directly, instead of calling the number provided on the received automated voice message.

BUYING THE PHARM

"Technology is making it so much easier to find this information and easier to do," Finley said. "You just have to use common sense."

Information such as maiden names, street addresses and driver's license numbers are all part of public record and a lot of companies pharm for identities, Finley said. Pharmed information is how companies tailor advertisements, mailings and other marketing tools to specific audiences. These companies use this information harmlessly, seeking only to enhance their marketability and reach those who >>

>> are most likely to be interested in their product. Unfortunately, they do not always choose to keep the information they pharm private.

"A lot of the people who have this information didn't get it illegally," Finley said. They got it from people you do business with online. Nine out of 10 companies these days sell their client lists to other people.

"They need money and sell their lists," he continued. "The problem is they don't always sell them to other legitimate companies."

Personal information can also be pharmed from hackers who redirect you from a legitimate website to an imposter site to harvest personal data. Social networking sites like Facebook and Twitter are increasingly being targeted in these scams.

Social networking sites are also places where people need to be careful about how much information they put out there. Information such as full birth date, geo tags on uploaded photos, maiden names, high school, family members and sometimes even addresses and phone numbers, easily found on social networking sites, give thieves ample information to steal an identity. People aren't thinking through what information they allow to be put out to their supposed "friends," DOCJT's McKinney said.

"We have a lot of kid victims — for a generation that is so technically savvy, they are so technically stupid," Finley said

“*The more information you make available, the more likely you are to be a victim of identity theft in any of its forms.*”

about the ways young people share information online. "Sometimes the technology goes far beyond the ability of people to use common sense. The more information you make available, the more likely you are to be a victim of identity theft in any of its forms. You have to be smart about it. ... Maintain control of your information.

"Facebook changes stuff all the time and their policy is you have to opt out, not opt in," Finley continued. "[You] have to check the settings almost daily to keep things hidden. For every one button you click, there's three back doors to get into that same thing. So, you have to check them all, all the time. Anything you put out there — well, if it's out there, it's out there forever."

I SPY ... SOMETHING STOLEN

Spyware is illicit software that can unknowingly be downloaded when an email attachment is opened, a pop-up window

is clicked or a corrupted song or game is downloaded. Sometimes the phishing emails sent out are harmless in and of themselves, Finley said. They don't ask the person to verify information, but when clicked on, a piece of spyware or malware downloads to the computer that logs key strokes and allows the thief to watch every move the user makes.

"Now they have all your passwords and log ins and they can get to all your accounts," Finley said. "They have full access to everything on your computer at that point. Some can even search your files."

Finley recommends purchasing good, reliable anti-virus software in order to prevent spyware identity theft. Having good software and being sure to keep it current can protect individuals from most of these types of unknown information theft on the computer. Software such as the Norton Security suite or Kaspersky cost approximately \$70 and can be placed on several computers, and cost an additional \$20 a year to keep current, Finley said.

"That's the best money you can spend if you're going to be online," he said. "It can scan and take that [junk] off and can block anything coming in and anything going out."

GOT MAIL?

With all the sophisticated computer scams out there these days, it may be easy to forget the simplicity of good old-fashioned pick pocketing, mail theft and people rooting through trash looking for information worth taking. There are lots of little steps individuals can take every day to protect their personal financial and account information from traditional forms of identity theft.

"A cheap insurance policy is a shredder," Finley said. "Make sure you get one

that can handle credit cards. You have to be very careful what you throw away. Even a piece of junk mail may look like a piece of random junk mail, but if you look, you may find there is a lot of your personal information on that."

"It may be in code, but the people that are stealing this stuff know how to use that code," Hopkinsville Detective Scott Raup added.

Making sure to shred all bills, credit card and bank account statements, and especially credit card offers received in the mail is a must to keeping identity thieves at bay. With the potential of numerous credit card offers showing up in someone's mailbox at a time, if simply thrown away, all a thief has to do is swipe them from the trash and change the address information, and he or she can receive a credit card in the victim's name in a snap.

The easiest way to detect identity theft is to monitor credit reports periodically, and not only at times when applying for financing for large purchases like a home or car, Raup said.

With three major credit-reporting agencies, Louisville Metro Police Detective John Mellen recommends taking advantage of the free credit report everyone is allowed once a year from each agency. By staggering when they are obtained, individuals can actually receive three free reports each year, one every four months, he said. Having consistent access to credit reports allows any fraudulent accounts to be noticed more quickly and be acted on more quickly, as well.

An identity theft case can take about a year to work from the initial report to adjudication, Mellen said.

"It takes a long time after that (to recover) — I don't think [the victims] ever get made whole, to be honest," Mellen said. "It's very hard to correct the damage that's done, especially if it is significant."

Making one's self aware of the types of identity theft out there, remembering to protect one's self through every available avenue and being proactive by checking in on one's own credit report intermittently can help anyone keep safe from identity theft and avoid the long-term effects of this crime. J

Abbie Darst can be reached at abbie.darst@ky.gov or (859) 622-6453.

Ten Things an Identity Thief Won't Tell You

Excerpts from Reader's Digest

1. That red flag tells the mail carrier — and me — that you have outgoing mail. That can mean credit card numbers and checks I can reproduce.
2. If a bill doesn't show up when it's supposed to, don't breathe a sigh of relief. Start to wonder if your mail has been stolen.
3. Why don't more of you call 888-5-OPTOUT to stop banks from sending you pre-approved credit offers? You're making it way too easy for me.
4. Even with all the new technology, most of us still steal your information the old-fashioned way: by swiping your wallet or purse, going through your mail or dumpster diving.
5. I never use my home computer to buy something with a credit card that's not mine. That's why you can often find me at the public library.
6. I can buy stolen account information — your name, address, credit card number and more — for \$10 to \$50 per account from hackers who advertise on more than a dozen black-market websites.
7. If you use the same ATM every time, you're a lot more likely to notice if something changes on the machine, like the skimmer I installed.
8. Hey, thanks for writing your pin number on that little slip of paper in your wallet. I feel like I just won the lottery.
9. Watch your back in line at the grocery store. I'll hold my phone like I'm looking at the screen and snap your card as you're using it. Next thing you know, I'm ordering things online on your dime.
10. My least favorite credit card is an American Express because it likes to ask me for your zip code. n



PHOTO BY ELIZABETH THOMAS



Take it

from me

One Kentucky chief's identity theft plight

ABBIE DARST | PROGRAM COORDINATOR

Twelve years ago, on a cool, blustery afternoon after arriving home from a long day at his department, he plucked the mail from the mailbox, kicked off his shoes and melted onto his sofa to rifle through the assortment of bills, letters and advertisements he'd received. Chief of a small midwestern U.S. city, this current Kentucky chief, who wishes to remain anonymous, was never vexed by this process, but was at peace with the security he had in knowing he had the ability to pay all of his bills.

"I'm a person who can't rest until my bills are paid," he said. "I've been very fortunate that the Lord has blessed me to have a job, and I've always been prompt on paying my bills. So, I never had creditors hounding me."

But this day, one of the letters he opened led him on a journey he never could have imagined. When he opened this particular letter from a random credit company, the words 'you owe us ...' seemed to scream out at him from the stark white paper. As he continued reading about how repeated attempts to collect had been unsuccessful and the debt was being turned over to a collection agency, he chuckled slightly as he prepared to toss the obviously mis-sent letter in the trash. But he paused.

"I thought, this has to be a mistake, I don't have a credit card here; I didn't do this," the chief said. "It's just a mistake and I'll straighten it out."

So, instead of pitching the letter, he called the credit agency to let them know he had received the erroneous letter and clear up the matter immediately. After being berated and accused by the person on the other end of the phone, he quickly realized there would be nothing immediate about this process.

"They threatened and said we're going to do this and that," he recalled. "I said, 'I'm trying to call and straighten it out, it's not me, I haven't done it.' They'd say, 'Well it's your social security number right ... then you're on the hook for it, so you have to make it good.'"

Flustered, irritated and completely caught off guard, the chief contacted the fraud section of the credit agency, which informed him he needed a police report and an affidavit in order to officially begin the process of clearing his name.

The chief then became even more concerned and decided to check his credit report and figure out exactly what was going on. He found five or six unknown open accounts on his report. >>

>> Despite having been a cop for nearly 30 years at the time, the chief had fallen victim to identity theft, one of the fastest growing crimes in America.

"There was all kinds of stuff on my credit report that I had no knowledge of — different credit cards and stuff," he said. "I had to go through each one and I had to argue with the guy they hire to try and scare you into giving the money over the phone.

"I think they got me for about \$40,000 and here I had no clue until I got this letter and it led me to the rest of it. It was a frightening experience because I thought I was doing everything right — hanging on to my credit cards, not giving them to my buddies, and this still happened to me."

The chief recalls the embarrassment he felt because he — the chief of police — fell victim to this type of crime.

"It's a little bit embarrassing because you're supposed to be the police and you're supposed to know how these things work, and they're not supposed to get you," he

said. "But it can happen to anybody. It doesn't matter what your rank. I thought I'd be the last person to even worry about it, but some of these people out here are very, very sharp and they know the system, and they know how it works."

After nearly two years, this now-Kentucky police chief was finally able to get all the fraudulent accounts closed and cleared up. Though he would never wish to go through this situation ever again, he said it was a good experience because it opened his eyes to the places he had left himself vulnerable.

"A lot of people would take it and say, 'this isn't me,' throw it away and go on about their business," the chief said. "But I've found it's better to do a little checking and make sure because it can impact you in a way you're not thinking about.

"It was a good experience," he continued. "It didn't cost me any money, but a lot of grief and time documenting everything — who you talked to, what date. It was a good

lesson. It taught me that watching your credit is very valuable."

To this day, the chief does not know how or where his identity thief picked up his information — he doesn't even know the thief's true identity. But his victimization put him on guard — ready for any future threats on his good name.

"I shred everything — I have a shredder at home and one here at the office," he said. "I check my credit report at least once or twice a year. ... I also don't do Facebook for a couple of reasons: 1) I don't have the time and 2) it's risky because that's just another piece of you that they have out there that they might want to try and do something with.

"It's frightening, it really is," the chief continued. "Especially when that's all a working man has is his credit. If you don't have your credit, you don't have anything." J

Abbie Darst can be reached at abbie.darst@ky.gov or (859) 622-6453.

A New Twist ABBIE DARST | PROGRAM COORDINATOR

The identity theft statutes in Kentucky seem pretty straightforward in how they can be used. A person has to use someone else's identifying information either with the purpose of financial gain or to avoid detection.

But detectives Scott Raup and Burt Finley of the Hopkinsville Police Department are using the identity theft charge in cyber-bullying cases.

After seeing students and other community members bashing each other on forum-type sites like Topix.com, they realized something had to be done to educate the public and raise the consequences for participating in forums where cyber bullying had become the norm, Raup and Finley said.

On many of these open forum sites, individuals can log on without registering and type in any screen name they choose. So, they found that students would enter these sites with a grievance against another student and do things such as use the other individual's name and say, "I'm gay," or "I'm pregnant," for example. However, by using someone else's name to hide their personal identification and avoid detection, it actually made what they were doing a form of identity theft, Finley said.

"So, it can get a little more serious than just your run-of-the-mill teasing and picking now," Raup said.

Hopkinsville detectives have been successful in using identity theft charges in multiple cyber-bullying cases, as well as using the potential for the charge as a deterrent when they provide educational presentations on the dangers of cyber bullying.

For more information, contact the Hopkinsville Police Department at (270) 890-1542. □

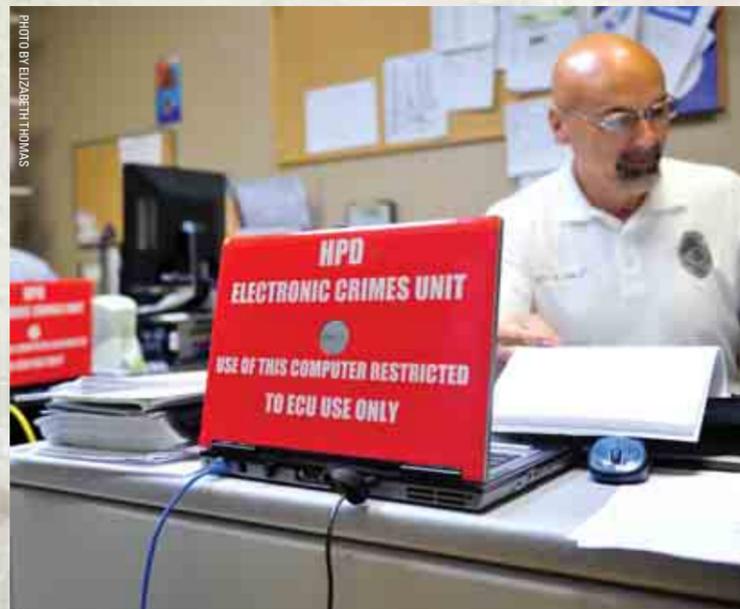


PHOTO BY ELIZABETH THOMAS

□ Hopkinsville Police Detective Burt Finley (pictured), along with Detective Scott Raup, are the two detectives assigned to the agency's Electronic Crimes Unit. The bright red labeled laptop covers identify the computers on which they work, so that other officers will not hook them up to the department network, allowing them to be traced as officers in the online world in which they conduct investigations.

Resources, Resources, Resources

For small, busy law enforcement agencies across the state there is a plethora of resources to offer victims of identity theft and to help with community education on how to avoid and detect identity theft. For information such as pamphlets, slide presentations and CDs, visit <http://www.ftc.gov/bcp/edu/microsites/idtheft/become-a-partner.html> or scan this QR code.



The Federal Trade Commission website encourages law enforcement agencies to offer identity theft victims as much information as possible to help them help themselves, therefore

helping them be the most cooperative with law enforcement. Below is a list of websites victims and officers can use to help with investigations.

U.S. Department of Justice

Request a free copy of the "Stop Identity Theft Now" educational video by calling (888) 228-0315. For more information: http://www.pueblo.gsa.gov/cic_text/money/idtheft_crooks/idtheft_crooks.htm

U.S. Secret Service Field Offices

http://www.secretservice.gov/field_offices.shtml

Electronic Crimes Task Force

Locate a task force at http://www.ectaskforce.org/Regional_Locations.htm

U.S. Postal Inspection Service

Locate your nearest postal inspection service and contact <https://postalinspectors.uspis.gov/>

E-Information Network

Access a unique collection of resource databases that help financial institutions and law enforcement obtain information on a variety of topics www.einformation.usss.gov

International Association of Chiefs of Police

www.theiacp.org

ID Safety Resources

<http://www.idsafety.org/enforcement/resources>

International Association of Financial Crimes Investigators

The Identity Theft Assistance Center is a cooperative private sector initiative that provides a free victim assistance service for customers of its member companies, and shares data with the Federal Trade Commission and other law enforcement agencies. Visit www.identitytheftassistance.org and www.iafci.org □

INTERACTIVE TOOLKIT
DETER · DETECT · DEFEND
AVOID THEFT
ftc.gov/idtheft

FIGHTING BACK AGAINST
IDENTITY THEFT
FEDERAL TRADE COMMISSION

HOW TO PLAN & HOST
PROTECT YOUR
IDENTITY
DAYS