



Police Beat

SCPD Crime Prevention Newsletter

Vol. 2 Issue 4

Dec. 2015

Felony Lane Gang strikes up and down Fox Valley

On Oct. 28, St. Charles police officers responded to a possible car burglary in progress at Goldfish Swim School off of Kirk Road. Once in the area, an officer spotted what was described as the suspect vehicle leaving the area and attempted to stop the vehicle. The vehicle refused to stop, fled the area at high rates of speed and eventually crashed in Bartlett. The offenders were arrested, and it soon was learned that they were part of a nationwide gang known as the “Felony Lane Gang.” The group is not so much a gang in the traditional sense, but multiple offenders acting in small, independent groups that commit car burglaries to steal checkbooks and IDs to make quick cash.

The idea was born in Fort Lauderdale, Fla. some 10 years ago. Offenders rent vehicles from that area and drive to communities across the country. They are known to target daycare facilities, preschools, parks, or any other place where women likely are to leave their purses in the vehicle as they run into a facility to drop off their kids.

They are known to physically break into locked vehicles as well. Male offenders will be in and out of a vehicle within a matter of seconds



Graphic zdnet.com

before they quickly flee the area. Any checkbooks that are located then are immediately given to female accomplices. They will write out a check to cash and disguise themselves to look like the females on the stolen driver’s licenses. Then they drive to a bank, usually in another city or even state, and utilize the furthest drive-thru lane (dubbed the “felony lane”) to make it more difficult for bank tellers to identify the driver. Just like that, your vehicle has been broken into and money will be missing from your account perhaps before you even walk back outside to your car. Offenders will then move to another city or state.

It’s a devastatingly easy routine that has made offenders literally mil-

lions of dollars over the years. Nearly every state in the union has been affected by this, and unless caught in the act like they were here in October, identification and prosecution is very difficult.

Another incident occurred during the first week of December at the Goddard School, a preschool located off of Kirk Rd. Since these incidents in St. Charles, communities from Montgomery to Algonquin have been hit with crimes directly related to the Felony Lane Gang. Surrounding counties also have been hit, as well as towns in central Illinois.

So, what can you do to protect yourself? Check out the information on the next page for details.

Protecting a child's info after a data breach

by Nicole Fleming
FTC Consumer Education Specialist

If you've ever had your information exposed in a data breach, you know it can be stressful. Depending on [what information is exposed](#), you might have to cancel credit or debit cards, change online passwords, or even put a freeze on your credit.

But what happens if your child's personal information is exposed, too?

An identity thief could use your child's social security number to get a job or a tax refund, open bank and credit card accounts, apply for a loan or rent a place to live. And what's worse, it might be years before you or your child realizes there's a problem.

So what can you do if your child's information is exposed? First, check to see if your child has a credit report. Generally, children shouldn't have credit reports — unless someone is using their information for fraud. Each credit bureau has its own process for checking:

[Equifax](#)

[Experian](#) — Click on "Minor Child Instructions" under "Information You Should Know"

[Transunion](#)

If your child has a credit report, follow the credit bureau's instructions for correcting fraudulent information. For help, visit IdentityTheft.gov or review the FTC's information about [child identity theft](#).

In [some states](#), even if your child doesn't have a

credit report, you can place a freeze that will make it difficult for someone to use your child's social security number to open new accounts. Each credit bureau has specific instructions for placing a freeze:

[Equifax](#)

[Experian](#)

[Transunion](#)

Even if you aren't aware of any problems, it's a good idea to check your child's credit history when he or she turns 16. That gives you time to fix any unexpected problems — before your child applies for a loan, an apartment, or insurance.

To learn more about what you can do when there's a data breach, visit IdentityTheft.gov/databreach.

DID YOU KNOW?

When you see words highlighted in text that means a web site address is embedded in the text. You can hit "shift" and the left button on your mouse to be taken directly to the web site in a new window.



Felony Lane Gang — how to protect yourself

- Do not leave ANY valuables inside of a locked or unlocked vehicle. If you have recent purchases in the vehicle, keep them out of view.
- Do not leave purses in the trunk. These offenders are known to watch victims as they put purses into the trunk of a vehicle.
- Lock your vehicle no matter where it is parked - even in your own driveway.
- Never leave your vehicle unoccupied with the key in the ignition and the motor running.
- Always make sure to park in a well-lit area.
- Pay attention to your surroundings in a parking lot. If you notice multiple individuals sitting in a vehicle for an inordinate amount of time, that is suspicious, and should be reported to the police by calling 911.
- Report to the police ANY incident in which you believe somebody has entered your vehicle, even if you did not experience a loss. Burglary offenders often are caught in the act, but without victims, offenders cannot be charged.



Preparation is key for winter driving survival

El Nino may keep a majority of the snow away this winter, but it never hurts to be prepared. Driving in the winter means snow, sleet, and ice that can lead to slower traffic, hazardous road conditions, hot tempers and unforeseen dangers. To help you make it safely through winter, here are some suggestions from the National Safety Council to make sure that you and your vehicle are prepared.

Your car

Prepare your car for winter. Start with a checkup that includes:

- Checking the ignition, brakes, wiring, hoses and fan belts.
- Changing and adjusting the spark plugs.
- Checking the air, fuel and emission filters, and the PCV valve.
- Inspecting the distributor.
- Checking the battery.
- Checking the tires for air, sidewall wear and tread depth.
- Checking antifreeze level and the freeze line.

Necessary equipment

An emergency situation on the roadways can arise at any time and you must be prepared. Following the tune-up, a full tank of gas and fresh anti-freeze, the following items should be in the truck of your car:

- A properly inflated spare tire, wheel wrench and tri-

pod-type jack

- A shovel
- Jumper cables
- Tow and tire chains
- A bag of salt or cat litter
- Tool kit

Essential supplies

Be prepared with a survival kit that should always remain in the car. Replenish after use. Essential supplies include:

- Working flashlight and extra batteries
- Reflective triangles and brightly-colored cloth
- Compass
- First aid kit
- Exterior windshield cleaner
- Ice scraper and snow brush
- Wooden stick matches in a waterproof container
- Scissors and string/cord
- Non-perishable, high energy foods like unsalted canned nuts, dried fruits, and hard candy

In addition, if you are driving long distances under cold, snowy and icy conditions, you should also carry supplies to keep you warm, such as heavy woolen mittens, socks, a cap and blankets.

What you need to know about chip-and-PIN

by [Sienna Kossman](#)
[Creditcards.com](#)

The nationwide shift to EMV (also known as chip-and-PIN) is well underway. EMV -- which stands for Europay, MasterCard and Visa -- is a global standard for cards equipped with computer chips and the technology used to authenticate chip-card transactions. In the wake of numerous large-scale data breaches and increasing rates of counterfeit card fraud, U.S. card issuers are migrating to this new technology to protect consumers and reduce the costs of fraud. For consumers, it means activating new cards and learning new payment processes. Most of all, it means greater protection against fraud.

Why are EMV cards more secure than traditional cards?

It's that small, metallic square you'll see on new cards. That's a computer chip. The [magnetic stripes](#) on traditional credit and debit cards store unchanging data. Whoever accesses that data gains the sensitive card and cardholder information necessary to make purchases. That makes traditional cards prime targets for counterfeiters, who [convert stolen card data to cash](#). Unlike magnetic-stripe cards, every time an EMV card is used for payment, the card chip creates a unique transaction code that cannot be used again. If a hacker stole the chip information from one specific point of sale, typical card duplication would never work "because the stolen transaction number created in that instance wouldn't be usable again and the card would just get denied," says Dave Witts, president of U.S. payment systems for Creditcall, a payment gateway and EMV software developer. Experts hope it will help significantly reduce fraud in the U.S., which has doubled in the past seven years as criminals have shied away from countries that already have transitioned to EMV cards.

Will I still have to sign or use a PIN for card transaction?

Yes and no. You will have to do one of those verification methods, but it depends on the verification method tied to

your EMV card, not if your card is debit or credit. Chip-and-PIN cards operate just like the checking-account debit card you have been using for years. Entering a PIN connects the payment terminal to the payment processor for real-time transaction verification and approval. However, many payment processors are not equipped with the technology needed to handle EMV chip-and-PIN credit transactions. So it is not likely you will have to memorize new PINs anytime soon, according to Conroy. As with a magnetic-stripe credit card, you sign on the point-of-sale terminal to take responsibility for the payment when making a chip-and-signature card transaction. Despite a slow transition overall, those

who get chip-and-PIN cards will be able to use them right away.

If fraud occurs after EMV cards are issued, who will be liable for the costs?

Today, if an in-store transaction is conducted using a counterfeit, stolen or otherwise compromised card, consumer losses from that transaction fall back on the payment processor or issuing bank, depending on the card's terms and

conditions. After an Oct. 1, 2015 deadline created by major U.S. credit card issuers MasterCard, Visa, Discover and American Express, the liability for [card-present fraud](#) will shift to whichever party is the least EMV-compliant in a fraudulent transaction. Consider the example of a financial institution that issues a chip card used at a merchant that has not changed its system to accept chip technology. This allows a counterfeit card to be successfully used. The major credit card issuers each have published [detailed schedules](#) about the upcoming shift in liability. The change is intended to help bring the entire payment industry on board with EMV by encouraging compliance to avoid liability costs. Any parties that did not meet the October deadline could face much higher costs in the event of a large data breach. Automated fuel dispensers will have until 2017 to make the shift to EMV. Until then, they will follow existing fraud liability rulings.



New credit cards means new scams

by Colleen Tressler

FTC Consumer Education Specialist

As discussed on the previous page, we told you about the [new credit and debit chip cards](#) designed to reduce fraud, including counterfeiting.

Unfortunately, as with anything new, scammers always will try to take advantage of the public's confusion, and misinformation. These scammers now are trying to take advantage of the millions of consumers who haven't yet received a chip card.

Here's what's happening: Scammers are emailing people, posing as their card issuer—be it their financial institutions or credit card companies. The scammers claim that in order to issue a new chip card, you need to update your account by confirming some personal information or clicking on a link to continue the process.

If you reply to the email with personal information, the scammer can use it to commit [identity theft](#). If you click on

the link, you may unknowingly install [malware](#) on your device. Malware programs can cause your device to crash, monitor your online activity, send spam, steal personal information and commit fraud.

So how can you tell if the email is from a scammer?

- There's no reason your card issuer needs to contact you by email — or by phone, for that matter — to confirm personal information before sending you a new chip card. Don't respond to an email or phone call that asks you to provide your card number. Period.
- Still not sure if the email is a scam? Contact your card issuers at the phone numbers on your cards.
- Don't trust links in emails. Only provide personal information through a company's website if you typed in the web address yourself and you



see signals that the site is secure, like a URL that begins https (the "s" stands for secure).

To learn more about protecting your personal information, check out [Privacy & Identity](#).

Third quarter police reports

The following information represents the number of reports taken by the St. Charles Police Department for the period July 1 through Sept. 30, 2015.

Commercial burglary - 5

Residential burglary - 2

Burglary from motor vehicle - 23

Motor vehicle theft - 4

Retail theft - 35

Identity theft - 20

Criminal damage to property - 34

DUI (alcohol and drugs) - 39

The city of St. Charles is social!

Keep up to date with all that's happening in St. Charles by following the city on these sites:



facebook.com/cityofstcharles



twitter.com/cityofstcharles



vimeo.com/stcharlesil



www.stcharlesil.gov