2016 CLM Annual Conference
April 6-8, 2016
Orlando, FL

"The Future of Fighting Fraud"

I. Introduction

The internet age has spawned a multitude of industries that has changed everything in our daily lives. From our means of communicating (or not) to how we travel, eat and receive information, we are in a time of incredible technological advancements.

The criminal element has also embraced the opportunities afforded by the advancement and widespread use of tech devices, and the insurance industry has seen the effects of cyber security breaches, identity theft and identity fraud become pressing issues along all lines.

With mobile pay, driverless cars, and 3D printing moving along from novelty ideas to mainstream usage, the opportunities for fraud will be even more prevalent. This presentation will cover how the developments in the technology are both presenting new challenges to the insurance industry as well as providing new opportunities for claims investigation.

II. Digital Disruption

In 2016, businesses are making it simple for us to use our mobile phones to do tasks like paying our bills. With the rise of conducting simple tasks like banking on our phone, credit card numbers, debit card information and social security numbers have become easily accessible to hackers.

Fake IDs are not being created anymore just for the purpose of an underage teen entering a bar. Fake IDs are an integral part of a modern day fraudulent scheme known as synthetic schemes. A hacker creates a fake ID to obtain credit cards from an individual, and diligently pays their bills for extended periods of time, which raises the credit limit of the cards. Once a certain credit limits is reached, the person who created the fake identity performs an activity called a "bust out" , where the person takes out a cash advance for almost the entirety of the credit limit and leaves town.

Other hackers have obtained credit card numbers from major retailers and social security numbers from other organizations. The hackers then contact the banks who issued the credit cards and change the pin numbers for the credit card accounts with the use of the social security numbers obtained. The

hackers put all of this data together, and sell it on the black market as re-issued debit cards, which purchasers can use to take money out of ATM machines.

Cyber attacks are very common. For instance, there were approximately 5 million detected cyber attacks in 2009. The number has risen drastically. In 2014, it was reported that there were as many as 40 million known cyber attacks. The average cyber breach costs a company on average $12 million dollars. The number of cyber attacks is on the rise despite the fact that most companies are investing more money and resources into security measures to combat cyber attacks.

III. Effect of Digital Disruption on the Insurance Industry

The rise of technology has not only had effects on the banking and credit card industries. The field of insurance has also been impacted by the rise of the use of technology like mobile apps. In the recent past, in order to obtain insurance, an applicant would have to go to an insurance agency to apply for insurance. The benefit of the face to face contact between the insurance agent and the insurance applicant is that the insurance agent could evaluate certain qualities of the applicant like truthfulness. Today, an online application is typically used to apply for insurance. In the near future, screening systems will be developed to analyze the identity of the applicant, and their insurance and loss histories. The development in screening systems would help compensate for some information that is lost when there is no face to face contact.

IV: Data Driven Investigations

Typically if a claims adjuster is alerted to suspicious activity during the investigation of a claim, the adjuster will refer the claim to the SIU unit. The SIU investigator uses investigative methods such as phone calls, and conducting interviews to collect additional information about the claim.

We anticipate that within the next 5 years, SIU investigations will look much different. A claims adjuster will be able to input a name into a system that will be able to search through multiple channels of information, for the purpose of identifying suspicious data and behaviors. We anticipate that these programs will be able to search through a variety of information including, social networking websites, news websites, weather data, telematics devises and satellite photography. This presentation will discuss the ways in which social networking websites, weather data, telematics devises and satellite photography can be important tools in the investigation of a claim and the defense of a lawsuit.

V. Discovery of Information on Social Media Websites during a Lawsuit

While the effects of the growing use of technology can at times, be negative, as demonstrated above, social media can be a beneficial tool for an insurance company to use in it's investigation of a claim. In addition to the rise of the use of mobile banking apps, almost everyone is using social media to provide information about themselves to the world. Facebook, Twitter and Instagram are currently some of the most popular social media sites. Often times, a claimant may be alleging that he or she has sustained a permanent injury as a result of an accident and is limited in the physical activities that he or she can participate in the future. However, often times, a claimant will post a picture or video of himself on a social media site after the accident which demonstrates, that the claimant

in fact, has no limitations on his or her ability to participate in physical activities. Investigation of a claimant's social media account additionally has the potential to provide information about potential witnesses to the accident or the motives of the claimant for filing a claim.

VI. Discovery of Social Media Accounts During Litigation

Discovery of content maintained on social media websites is permitted under the Federal Rules of Civil Procedure. Pursuant to Federal Rule of Civil Procedure 34(a)(1)(A), a party may serve on any other party a request within the scope of Rule 26(b):

> 1. to produce and permit the requesting party or its representative to inspect, copy, test, or sample the following items in the responding party's possession, custody, or control:
>
>   a. graphs, charts, photographs, sound recordings, images, and other data or data compilations— stored in any medium from which information can be obtained either directly or, if necessary, after translation by the responding party into a reasonably usable form.

The case law on the discovery of a plaintiff's social media accounts is relatively new. Many challengers to the discovery of content available on social media account have raised the argument that privacy concerns outweigh the relevance of any content contained on a social media website, and therefore, discovery should not be permitted. This argument has been rejected by the Courts. For instance, in *Romano v. Steelcase, Inc.*, 907 NYS 2d 650 (N.Y. Sup. Ct. 2010) the Court found that since social networking websites such as Facebook and MySpace do not guarantee a user's right to privacy, there is no reasonable expectation of privacy in the content posted on social media websites. Further, the Court found that any privacy concerns
are outweighed by a party's right to discover all non-privileged and relevant materials. In this case, the Court found that pictures of the plaintiff outside of her home with a smile were directly relevant to plaintiff's claims that she could not leave her home as a result of an accident.

Additionally, in *Reid v. Ingerman Smith LLP*, CV 2012-0307 ILG MDG, 2012 WL 6720752 (E.D.N.Y. Dec. 27, 2012), the Court held that although a user may restrict access to his or her social media site to others in his or her network, there is no expectation that those who
access content on someone's social media site will not share the content with a user who is outside of the user's network. Therefore, the Court found that privacy concerns would not restrict access to the plaintiff's Facebook page, even when the plaintiff had privacy settings on her account which provided access to only her "friends". The Court added that content posted on social media sites is particularly relevant in personal injury cases in which the plaintiff is seeking future damages.

In *Higgins v. Koch Dev. Corp.*, 3:11-CV-81-RLY-WGH, 2013 WL 3366278 (S.D. Ind. July 5, 2013). In this case, the Court rejects the plaintiffs' argument that they have an expectation of privacy in their Facebook accounts simply because they have placed privacy restrictions on their accounts, such as

preventing certain people from viewing their accounts. The Court further rejected plaintiffs' arguments that discovery of their Facebook pages violates the privacy of non-parties to the action who posted on plaintiffs' Facebook accounts. The Court found that the content was relevant to plaintiffs' claimed respiratory injuries.

In *McMillen v. Hummingbird Speedway*, Case No. 113-2010 CD (Pa. Ct. of Common Pleas) (Sept. 9, 2010), the defendant sought discovery of the plaintiff's social media content by requesting the plaintiff's log in names and passwords for all of the plaintiff's social media accounts. In this case, the Court ordered the plaintiff to provide usernames and passwords for Facebook and MySpace accounts. The Court found that there was no claim of privilege, such as the attorney-client privilege, that would protect the disclosure of the username and password for social media accounts. Additionally, the Court reviewed the user agreements for Facebook and MySpace and found that there is nothing in the user agreements that suggest that the user is entitled to a confidentiality protection.

VII. Admissibility of Social Media Content at Trial

It appears that by far, most courts are permitting the discovery of the content contained on a social media website. This raises the question of whether information obtained through discovery on a plaintiff's social media account is admissible at trial. A few Courts have found that social media content can be authenticated like all other internet postings, via content and context. In *Tienda v. State*, No. PD-0312-11, 2012 Tex. Crim. App. LEXIS 244 (Tex. Crim. App. Feb. 8, 2012), the trial court allowed the jury to determine whether the appellant created the content of social networking pages based upon circumstantial evidence and admitted electronic content obtained from the social networking pages. According to the Court, "Any serious consideration of the requirement to authenticate electronic evidence needs to acknowledge that, given the wide diversity of such evidence, there is no single approach to authentication that will work in all instances."

VIII. The Future of Technology in Claims Investigations

On the rise in mobile devises and car technology is telematics. Telematics is a term that refers to any device which merges telecommunications and infomatics. Examples include GPS Systems and navigation systems.

Some examples of telematics that many of us are familiar with are OnStar and hands free mobile calling in the car. Telematics are a range of different features, options and devices that are brought together by a single principle – data and communication.

Telematics can also be useful for insurance companies. When telematics devises are installed in cars and other vehicles, they transmit data. In the future, we will see insurance companies utilizing these devises to monitor their insureds. For instance, telematics devices could provide information about the location of an insured at a given time and information regarding the manner in which the insured is operating the vehicle. Insurance Companies would gain insight into information that is largely unknown at this time, like whether an insured is regularly driving his or her vehicle in the location where the insurance policy was issued. Additionally, telematics devises could provide information in auto accident

investigations about the speed at which the car was driven and could provide clues about whether the car was being driven in a reckless manner.

A common problem in the investigation of auto accidents is that the investigation typically relies on the memory of eye witnesses. An eye witness account of an accident is not always reliable. However, insurance companies can now rely on smart phone telematics, like photographs, which can provide an accurate report on the conditions that were present at the time of accident.

Developments in the area of satellite photography will become even more useful in the evaluation of property damage claims as time goes on. . Image resolutions are getting much sharper, and there have been many developments in the range of images available. We anticipate that investigation of property damage claims could involve accessing high resolution photographs of the property before and after the loss. Currently, insurance companies are using drones to map the roofs of insured properties to evaluate roof damage claims. Additionally,
infrared technology is being used to access water damage claims by identifying cool spots. These technologies will provide valuable information about the condition of the property with and without the need for active field inspections.

.