



# MIGNOLET

BUSINESS RESEARCH CONSULTANTS, INC.

## In This Issue

Mastercard kicking  
Smartphone Fraud  
Facebook Fakes



For more than three decades Jean Mignolet has served in law enforcement and private investigation, managing all aspects of general investigative business. She specializes in in-depth background investigations, and is the top choice of attorneys, corporations, small business owners and individuals who require all types of investigative services.

For further information visit: [www.Mignolet.com](http://www.Mignolet.com)

Contact us at:  
[investigators@Mignolet.com](mailto:investigators@Mignolet.com)  
or call us at: 954-523-8737

**Quick Links**  
[Our Website](#)

Jean,

One of the most significant threats we face today is our **cyber security** states Lori Schiff Montgomery, Vice President of Corporate Insurance Advisors, LLC in Fort Lauderdale, Florida.

According to former Secretary of Homeland Security Michael Chertoff, all businesses that utilize computers or any advanced technology should consider cyber liability insurance policies, which can be written to include first and third party theft, data breach, extortion, virus coverage, etc. Chertoff strongly suggests that this type of Cyber Insurance Policy be considered.

According to Ms. Montgomery, you might also consider the following:

- Employee dishonesty - theft of money, securities or property by your employees;
- EPLI (employment practices liability) - covers for wrongful termination, sexual harassment, discrimination (can be extended to include defense for wage and hour.
- Fiduciary liability - pays for legal liability arising from claims for alleged failure to prudently act within the meaning of the Pension Reform Act of 1974.

Although there are literally thousands of insurance coverages and types of policies available, and this list is by no means

[Services](#)

[Join Our Mailing List!](#)

## MasterCard kicking fraud in the smartphone



What credit card company isn't looking to obliterate fraud so that they and their customers aren't losing billions of dollars? Worldwide the fraud reaches approximately \$5.55 billion and its rising. Even cards that are thought to be compromised lead to great losses. Cards at risk run up the tally another \$172 million plus. MasterCard made an announcement stating that they have partnered with a mobile technology company called **Syniverse**, to minimize unauthorized purchases. Syniverse is a mobile technology company with whom MasterCard is currently put into

complete, those mentioned above have, in recent years, become increasingly important to the majority of businesses. Call Ms. Montgomery at 954-314-5000, ext.123, if you have any questions about this type of insurance coverage to better protect your business and its assets.

*Jean Mignolet*

*A reminder that prior issues of the newsletter are viewable from [my website](#).*

## Facebook: 67 million FAKE accounts



Facebook has revealed that it has close to 760 million daily active users and that number is increasing by 22 percent each year. They show earnings of \$1.23 billion each quarter from monthly active users. Nearly 950 million of those monthly users access Facebook from their mobile devices.

Although this sounds impressive, the Company's very own 10-K filing shows that due to a number of fake accounts the numbers may not be accurate.

Facebook stated it was due to the following issues:

- Facebook estimates that between 4.3% and 7.9% of its monthly active users were individuals signing in with more than one account, despite the fact that duplicate accounts are against its terms of service.
- A further 0.8 percent to 2.1 percent of monthly users are believed to have been using misclassified accounts, used to represent something other than a real human user, i.e. accounts created for pets, businesses or organizations.
- Some 0.4 to 1.2 percent of accounts are said to be 'undesirable' because they have been

action an opt-in-pilot scheme allowing users to make transactions only when their mobile devices are on. You would then hand in a specific location where the purchase was made. All of that information then gets cross-checked and location of the mobile device AND the credit card must match. If you don't have your mobile with you at the time of the purchase, your purchase will be denied. Therefore, if your card is stolen and being used in Omaha and you are in Skiing in France; the purchase will be denied.

Joe DiFonzon, chief technology officer of Syniverse stated, "As soon as a mobile phone connects to the phone network we can see a user's location within milliseconds, just by which mobile phone mast they connect to and it is unspoofable, as we get the data directly from the back end of the network." MasterCard and its customers should benefit from this new technology because it will simply make it much more difficult for criminals to

created to violate Facebook terms of services by, for example, being used to send spam messages or other types of malicious links or content.

They also seek to identify "false" accounts, which they divide into two categories:

- (1) User-misclassified accounts, where users have created personal profiles for a business, organization, or non-human entity such as a pet (such entities are permitted on Facebook using a Page rather than a personal profile under their terms of service)
- or
- (2) Undesirable accounts, which represent user profiles that we determine are intended to be used for purposed that violate their terms of service, such as spamming.

**This information suggests that between 5.5% and 11/2% of all accounts on Facebook are either duplicate, malicious or otherwise 'fake' accounts.**

Based on their own figures, there are **at least 67 up to 137 million monthly users who are not who they purport to be...**Oddly enough, the US and UK are less prone to these fake accounts. Facebook believes geographical differences in the duplication, plays a large part.

There is no exact science in estimating how many fake accounts there actually are. At this time, they are basically relying on human judgment. And with such limitations such as user age data and other figures their estimation remains just that; an estimate.

utilize a stolen or cloned card.

As an appetizer, MasterCard is to offer a prepaid data package at specific popular destinations so their customers will not be put off from using the service by roaming data charges. **This is a great anti-fraud action and wonderful technology; however, the two companies will now know where you are at all times. This offers them an opportunity to make money from wherever you are.**

Mobile network operators and brands can also benefit from the collaboration between MasterCard and Syniverse. In the future, they could **implement targeted offers**, which will be made more relevant by knowing the location of a mobile device, for example in close proximity to a retail store. A research report for Syniverse from economists at SEEC uncovered a market valued of as much as \$44 billion for operators providing services to brands based on opted-in mobile subscribers' information...

This is an opt-in mobile subscriber action but it remains unclear what the

**So the bottom line is to be aware that you may be dealing with fake accounts. Double check everything before you purchase, talk to, or exchange information. Facebook doesn't know whether the number of fake accounts is growing or shrinking so have chosen to present a range of variables.**

The company's first earnings report gave a more precise figure of 8.7%, which equated to 83 million accounts. **Now who knows what the real numbers are?**

two companies have in mind for their own customers. Here's hoping they will resist the urge to *share their customers' location data by default.*