FOR IMMEDIATE RELEASE

Silicon Valley Cybersecurity Firm Wins Patents to Reduce Business Email Compromise

Palo Alto, California – November 13, 2018 – ZapFraud Inc, a Silicon Valley Cybersecurity Firm addressing targeted email attacks, was granted two foundational patents today on how to detect and address deceptive email attacks, such as spear phishing and Business Email Compromise (BEC).

At the heart of spear phishing and BEC attacks is the use of identity deception, more than 90% of which involves a technique referred to as "deceptive display names", wherein a criminal poses as a trusted party by sending an email with a display name matching the name of the trusted party. Commonly deployed security technologies such as spam filters and DMARC do not protect against these attacks, and security awareness campaigns have not shown any meaningful results.

"Criminals understand that almost no one tells from whom an email comes by looking at an email address, character by character. Instead, people look at the sender's name and the context of the email. If there are no immediate flags, one assumes the email to be authentic. This is how people fall victim to BEC attacks. These two patents automate the detection of deceptive messages, which will significantly decrease the risk of BEC," said Dr. Markus Jakobsson, founder of ZapFraud.

ZapFraud Patents 10,129,194 and 10,129,195 are two in a series of patents addressing identity deception. They describe how to detect deceptive messages based on automatic analysis of identity indicators, such as display names. ZapFraud plans to license the technology.

"ZapFraud understood the problem of spear phishing and Business Email Compromise before these attacks even had a name", said Professor Dan Boneh, an early investor in ZapFraud, and professor of Computer Science and Electrical Engineering at Stanford University and co-director of the Stanford Computer Security Lab.

Boneh explains that the key to the foresight of ZapFraud was the early work of its founder, Dr. Markus Jakobsson, in social engineering, online deception and targeted attacks.

Spear phishing attacks, such as the 2016 attack on the Democratic National Committee, are increasingly targeting U.S. businesses and institutions, and are used to exfiltrate sensitive data. BEC attacks are commonly used to persuade organizations to wire funds and to send sensitive information, such as W2 data, to criminals. According to the FBI, more than $12 Billion has been lost to BEC since 2013.

###

About ZapFraud
ZapFraud has an extensive portfolio of patents and pending patents addressing phishing, email deception, Business Email Compromise. Its founder, serial entrepreneur Dr. Markus Jakobsson predicted, in 2005, the development of targeted attacks using identity deception and began working on building countermeasures. In late 2011, in anticipation of the imminent development of threats such as Business Email Compromise, he laid the foundations to ZapFraud. For more information visit www.zapfraud.com.

For more information contact:
Liz Fuller
Lfuller@gardcommunications.com
503-552-5067