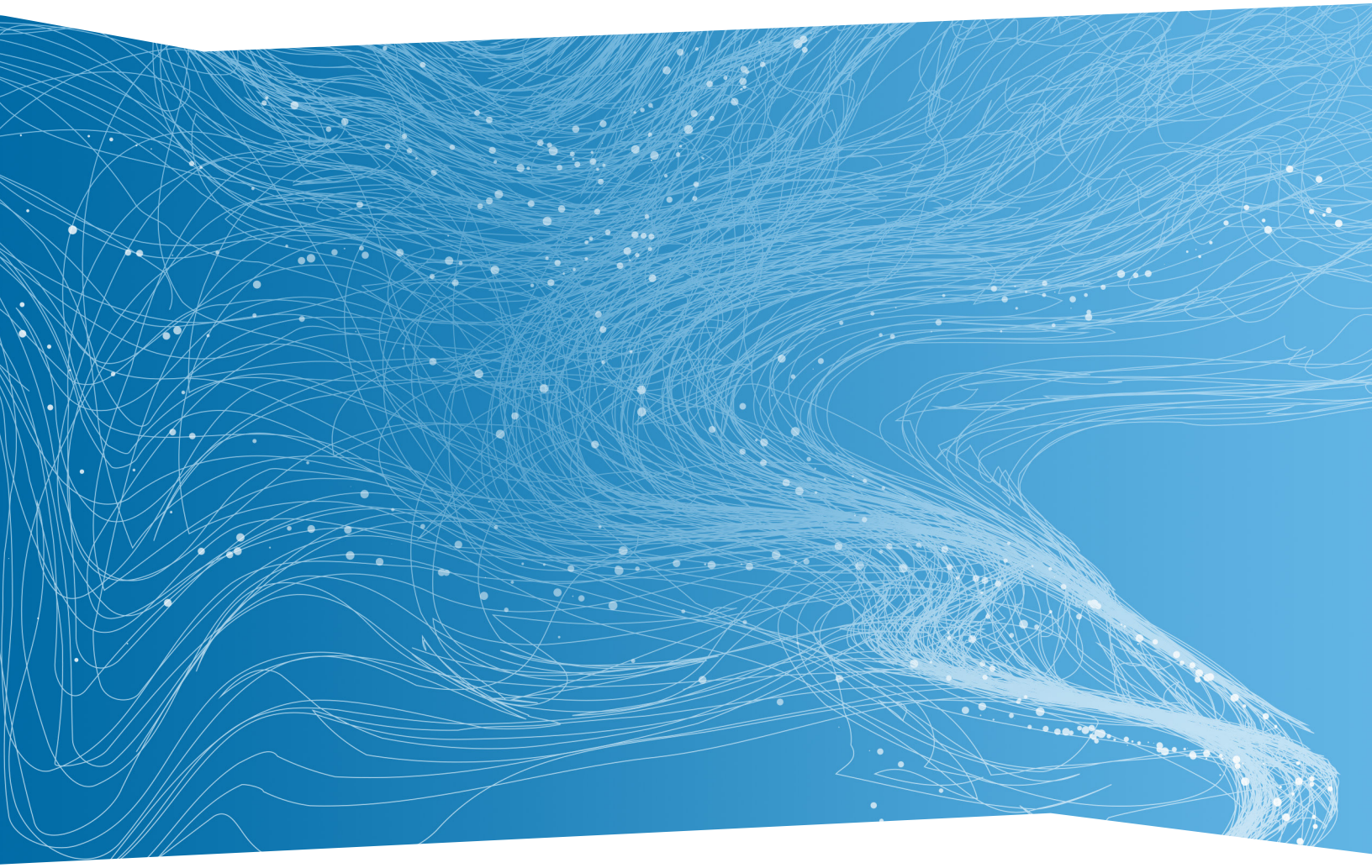
RSA



WHITE PAPER

THE SOCIAL MEDIA FRAUD REVOLUTION

A STUDY OF THE EXPANSION OF CYBERCRIME TO NEW PLATFORMS

RSA

Social media platforms have become one of the most visible and fastest-growing technologies in the last decade. The 24/7 availability and access, helped along by the use of smartphones, has made social media an integral part of our daily lives.

After releasing our extensive research, "Hiding in Plain Sight," in 2016, which highlighted the increasing spread of cybercrime activity on social media, RSA has continued to follow the evolution of fraudsters' use of these platforms to conduct their business. RSA has found that fraudsters have expanded their use of social media as well as extended their presence to many newer platforms.

Fraud groups in social media can be described as a uniform sphere, with fraudsters often advertising groups and contacts in multiple social networks and alternating between two or more platforms during a single conversation. Moreover, the content shared in the various social media groups is inherently similar and mainly serves to increase a fraudster's reputation and exposure.

While many fraudsters use social media as a gateway to the underground, reaching fraud forums through adverts they come across, in some countries fraudsters use it as their main fraud platform for communicating, much like darknet forums are used in other countries.

The RSA FraudAction Intelligence team monitors tens of thousands of accounts and groups that partake in financial fraud. The content ranges from screenshots of compromised and mule bank accounts through carded e-commerce orders to fraudsters trading cashout methods, fraud tools and techniques.

In this report, we will provide an overview of the predominant social media platforms where RSA has observed fraudulent activity, looking at the advantages and special characteristics of the specific media platform.

FACEBOOK

Facebook is the number one social media website today with over one billion users, setting the bar for all other social media networks.

Due to the enormous popularity and diverse user base, fraudsters' activity on Facebook continues to thrive, making it one of the most prominent platforms for fraud. Since RSA published "Hiding in Plain Sight" in 2016, fraud groups using Facebook have continued popping up and their member counts continue to grow significantly. Several of the more established fraud groups contain tens of thousands of members.

Prominent fraud groups utilize Facebook's marketplace feature, which provides them a convenient platform for trading fraud-related goods and services, all without leaving Facebook.

Consistent with other social media platforms, Facebook has introduced the Stories feature, which has been increasingly adopted by fraudsters. More

on Stories can be found under the Instagram and Snapchat sections in this report, both of which are highly associated with this feature.

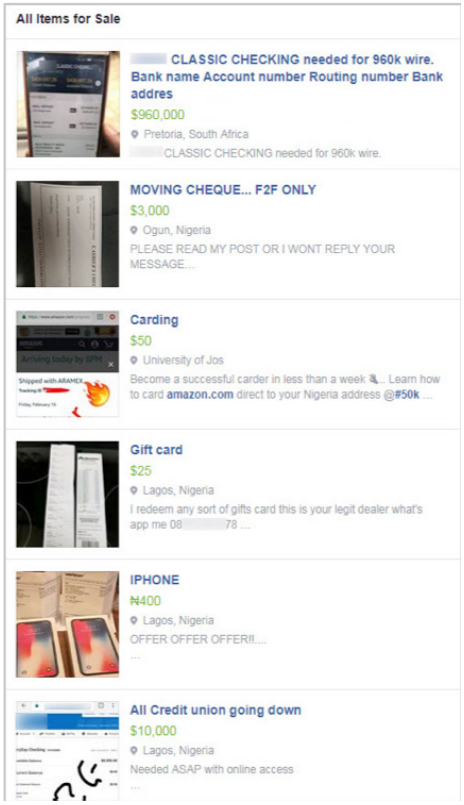
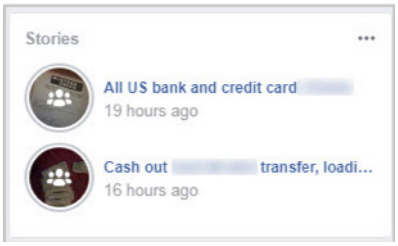


Figure 1: Facebook Fraud Group's Marketplace



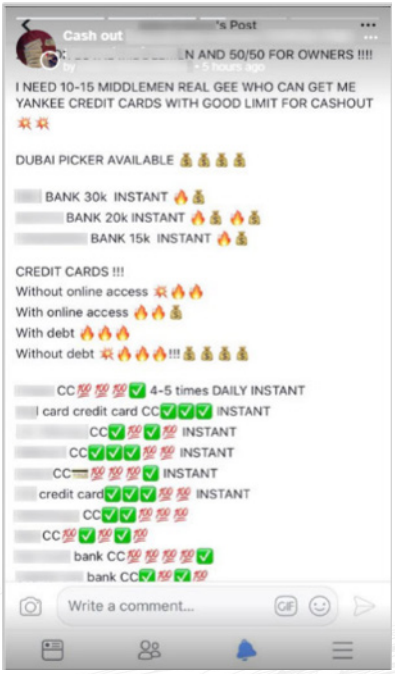


Figure 2: Fraudsters' "Stories" on Facebook

ICQ

ICQ is considered one of the most popular platforms used today by fraudsters, and in fact, the registration for many fraud sites requires an ICQ account number.

ICQ has served as fraudsters' traditional communication platform for peer-to-peer communication and live calls for years. Over time, fraudsters started forming groups which gradually increased in number and size. Today, there are countless fraud groups, and since ICQ does not limit their size, some contain thousands of members.

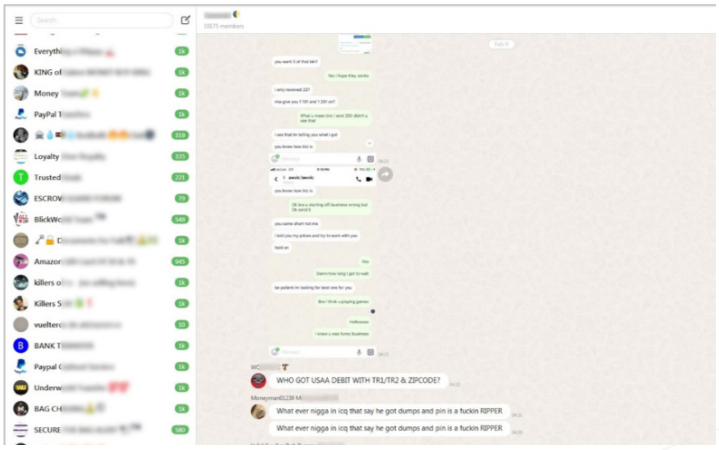


Figure 3: Fraud Groups on ICQ

WHATSAPP

WhatsApp, acquired by Facebook in 2014, is a widely adopted messaging app that hit over one billion users in 2017, making it yet another popular platform among fraudsters globally.

Beyond instant peer-to-peer messaging, WhatsApp serves fraudsters primarily for the purpose of disseminating information to numerous people at once. Since WhatsApp groups are limited to 256 members, fraud groups on this platform are many, making the prominent ones very exclusive. Fraudsters who are not active enough in a group are quickly removed.

After WhatsApp introduced its end-to-end encryption, it became even more appealing to fraudsters, providing them a safe haven to conduct their business.

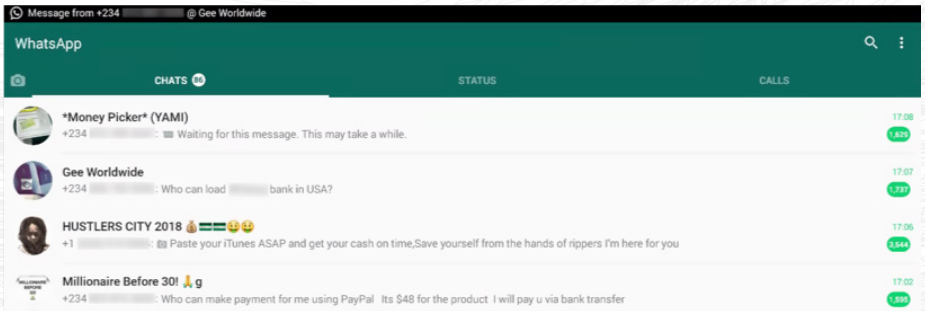


Figure 4: Fraud Groups on WhatsApp

RSA

TELEGRAM

While many fraudsters prefer WhatsApp due to its sheer popularity, a few who are more concerned with keeping their identity safe will choose Telegram, as it's perceived by some in the fraud community as more secure.

However, the main reason for choosing Telegram is the support of up to 100,000 members in a "supergroup," as well as the "channel" type of groups, which allows the admin to broadcast public messages to an unlimited number of people without the ability of regular members to send messages.

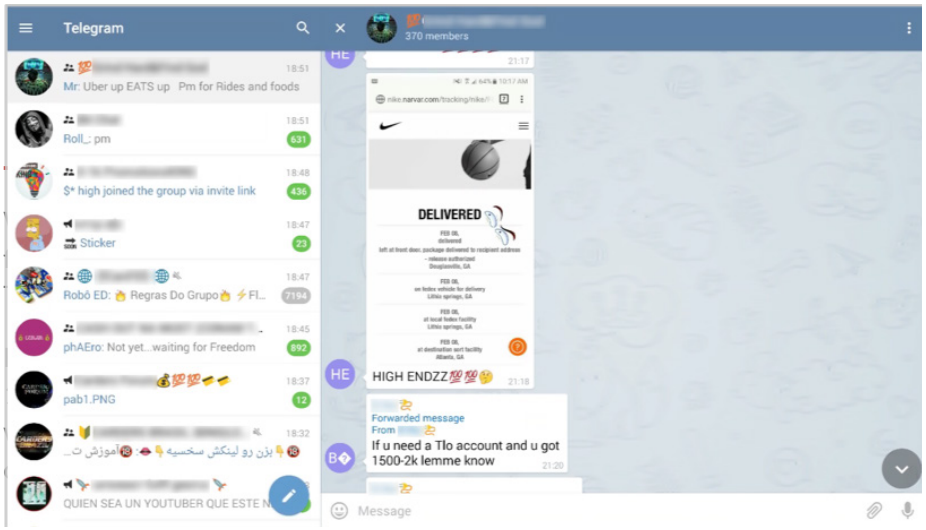


Figure 5: E-commerce Fraud Discussions in a Telegram Group

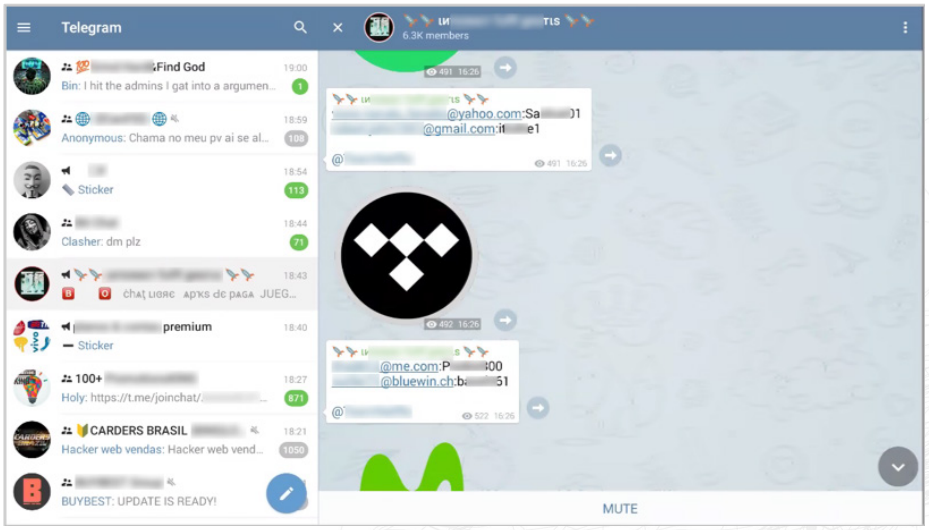


Figure 6: Telegram Fraud "Supergroup" Recognized by the Megaphone Sign to the Left of the Group's Name

RSA

INSTAGRAM

Instagram is a photo-sharing application that allows users to share images and videos either publicly or privately to pre-approved followers. Fraudsters on Instagram tend to follow each other and engage in private chats rather than form groups.

They use this platform to advertise their products and services by sharing proof of carded products from e-commerce sites, screenshots of cashed-out compromised bank accounts and more.

Its Stories feature allows the sharing of images and videos for a limited time frame, keeping them available only for 24 hours. This makes it even more appealing, as it creates a hype among fraudsters who are afraid to miss out on the opportunities that may lie in the advertisements.

Instagram recently introduced a new feature for sending photos or videos, which disappear immediately after viewing.

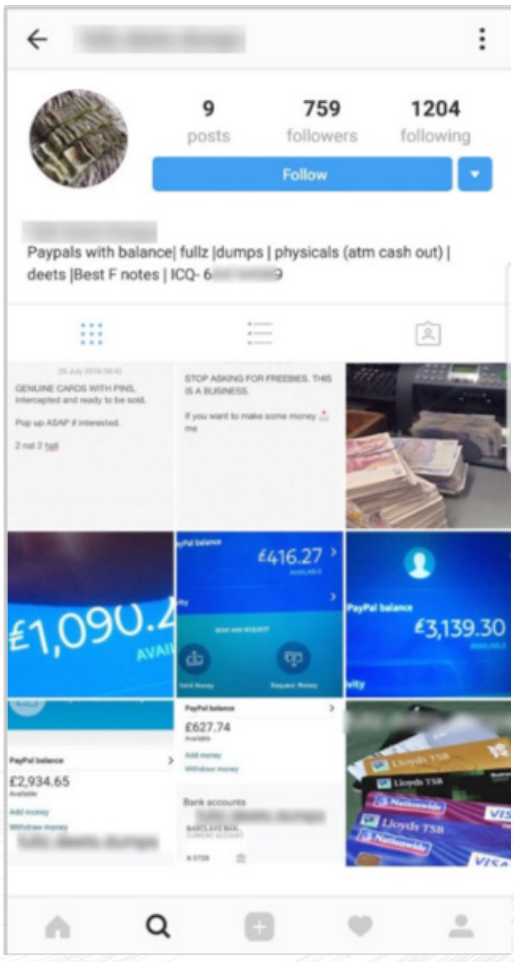


Figure 7: A Fraudster Advertises Payment Services Fraud in Instagram, Posting His ICQ Number for Contact

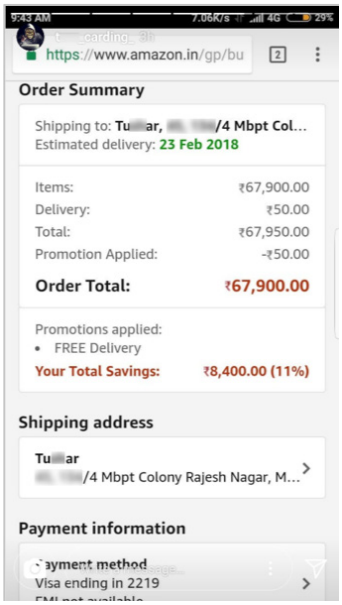


Figure 8: A Fraudster's Story Featuring a Carded Order on Instagram

SNAPCHAT

Snapchat is also an image messaging application that offers a Stories feature. It is most identified with its disappearing messages feature, as well as images and videos which disappear up to ten seconds after they are opened. While other platforms, such as ICQ and WhatsApp, enable the deleting of messages after they are sent, Snapchat automatically removes all messages after exiting the chat. Users are even notified if someone takes a screenshot of what they posted.

Despite the lack of end-to-end encryption, the above features allow fraudsters to communicate in a secretive manner.

While Snapchat does support small groups of up to 32 members, fraudsters typically prefer to use this platform for peer-to-peer messaging. Fraudsters often post their Snapchat IDs on Facebook in order to continue a private conversation.

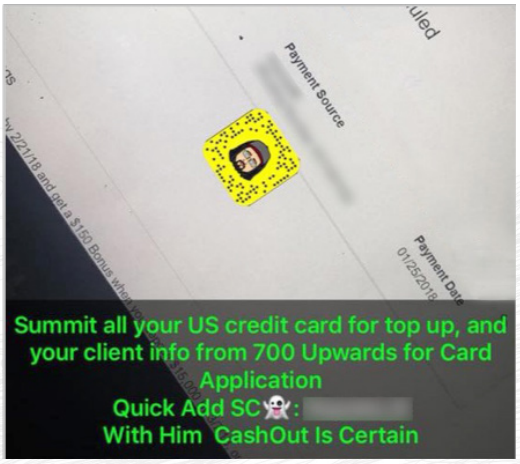


Figure 9: A Fraudster Marketing His Merchandise on Facebook Provides His Snapchat Account as a Means of Contact

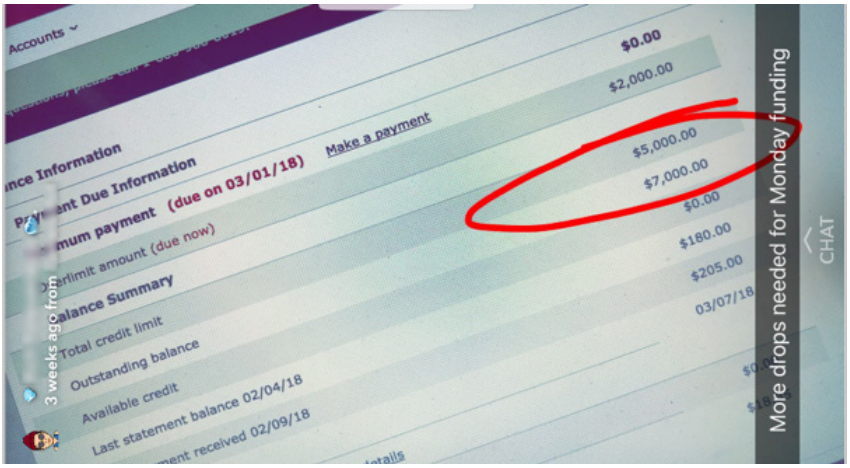


Figure 10: A Compromised Bank Account Screenshot Being Shared on Snapchat

REDDIT

Reddit is a collection of entries submitted by its registered users, essentially a bulletin board system. Each forum dedicated to a specific topic on the website is called a "subreddit."

Fraud subreddits and their active users are constantly banned, making it more difficult for fraudsters to maintain a healthy community. However, there are currently around 50 subreddits where fraudsters discuss fraud methods, look for partners and share knowledge. It is used less for advertising and sharing screenshots of fraudulent activities.

As Reddit is more popular in English-speaking countries, fraudsters using it typically speak English, contrary to other social media platforms.

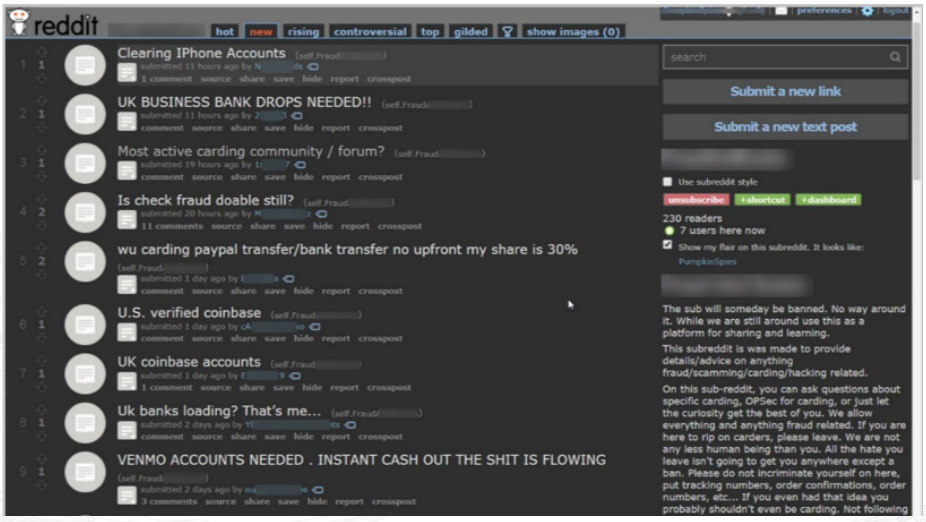


Figure 11: Fraud Subreddit Acknowledgment That Some Day It Will Be Banned Appears on the Bottom Right

YOUTUBE

YouTube is very popular among fraudsters and is used mainly for uploading videos for advertising and training. These videos will typically appear among the first search results presented when searching for fraudulent terms on Google. In addition, posted videos have a tendency of staying on YouTube for long periods, which fraudsters use to their advantage.

It is common to see tutorials of fraudsters demonstrating how to use a credit card checker or a certain skimmer that they sell. While fraudsters tend to recycle their advertisements and materials across many platforms, the content they advertise on YouTube is more distinct since it allows them to illustrate in more detail.

To gain more exposure, fraudsters often include links to their YouTube videos in posts on fraud forums, and vice versa, advertising their fraud websites on YouTube.

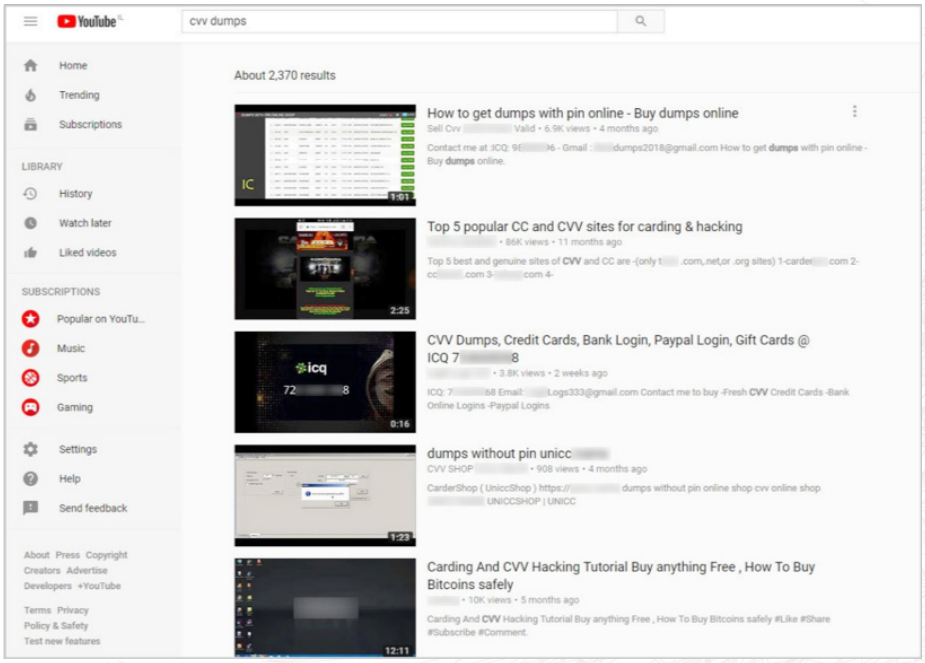


Figure 12: A Sample of Fraud Tutorials Related to Carding on YouTube

TWITTER, LINKEDIN, GOOGLE PLUS AND OTHERS

While not preferred among fraudsters for communication, RSA has observed various fraud activity occurring on platforms such as Twitter, LinkedIn, Google Plus and others.

These platforms may appeal less to fraudsters due to a variety of reasons that have to do with monitoring policy, level of popularity and common use.

Figure 13: A Fraudster Selling Compromised Card and PII Data on Twitter

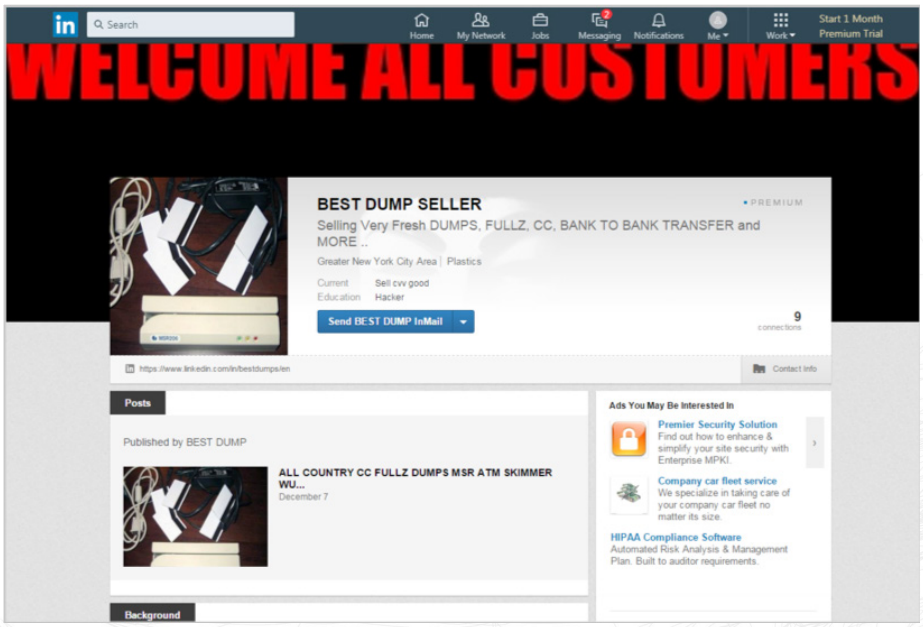


Figure 14: Skimmers, Compromised Card Data and PII for Sale on LinkedIn

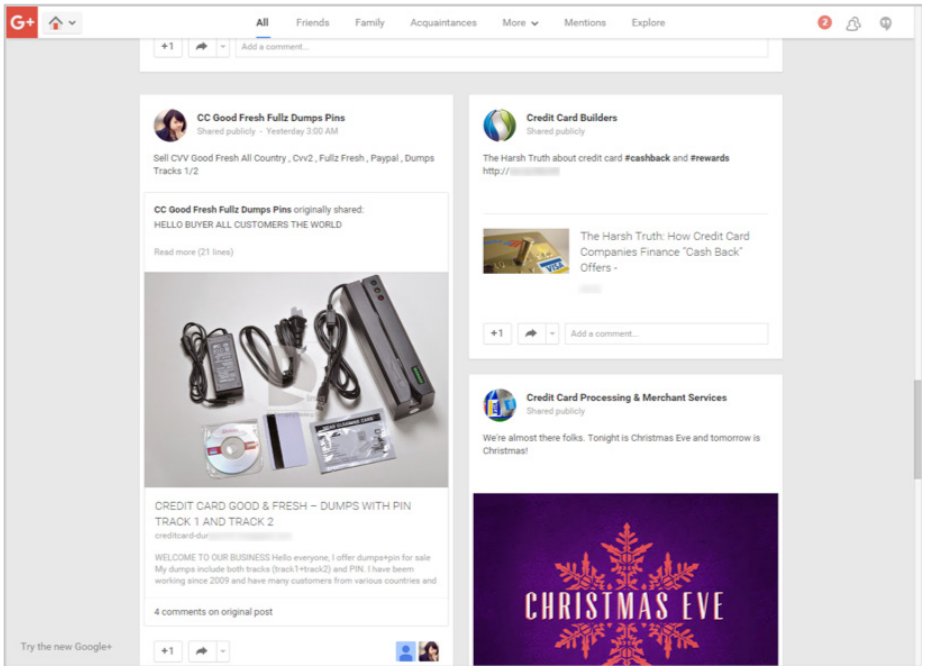


Figure 15: "Dumps" for Sale on Google Plus

CONCLUSION

The shutdown of large fraud marketplaces, including Infraud, AlphaBay Market and Hansa Market, combined with the rise in popularity of social media across the globe, has resulted in many fraudsters extending their presence on social media beyond Facebook to a much wider variety of platforms, including WhatsApp, Telegram, Instagram, Snapchat and others.

While some of the social media platforms offer many common functionalities, such as a Stories feature, encryption and "channel" groups, the way in which fraudsters utilize each platform varies based on their perception of that media, its popularity and adoption in their reigon, and their own personal preference.

In general, fraudsters try to be on as many platforms as possible in order to reach a wide and diverse audience. The names of the fraud groups themselves are sometimes generic, such as "Trusted Deals," and other times indicative of a specific type of fraud, such as "Swipe university" or "Ripper exposer."

An interesting observation to note is the line between instant messaging platforms and social media has blurred over the past few years. Today, fraud communication and advertising often occur within large groups, in which thousands of messages are shared every day. All of this serves as a fertile environment for a vibrant and dynamic fraud community to flourish, a trend that RSA will continue to monitor and report on.

RSA

ADDITIONAL RESOURCES

To view the RSA original research, "Hiding in Plain Sight," on the study of global cybercrime in social media, refer to the additional resources below.

Hiding in Plain Sight: Part 1
Part 1 of the series highlights the global presence of cybercrime on Facebook across multiple regions.

Hiding in Plain Sight: Part 2
Part 2 of the series highlights the presence of cybercrime specifically on Russian- and Chinese-speaking platforms.

Cybercrime in Social Media Grows 70% in Six Months
This article highlights the rapid growth of the use of social media by fraudsters and is a follow-up to the original Hiding in Plain Sight research.