RSA BUSINESS-DRIVEN SECURITY™

RSA QUARTERLY FRAUD REPORT

Volume 2, Issue 3
Q3 2019

CONTENTS

EXECUTIVE SUMMARY

The RSA® Quarterly Fraud Report contains fraud attack and consumer fraud data and analysis from the RSA Fraud and Risk Intelligence team. It represents a snapshot of the cyber-fraud environment, providing actionable intelligence to consumer-facing organizations of all sizes and types to enable more effective digital risk management.

RSA-OBSERVED FRAUD ATTACK AND CONSUMER TRENDS

For the period starting July 1, 2019, and ending September 30, 2019, RSA observed several global fraud trends across attack vectors and digital channels. The highlights include:

Phishing accounted for 43 percent of all fraud attacks observed by RSA in Q3. Overall, phishing volume has increased 57 percent as compared to the same time last year.

Canada remained the top targeted country in Q3, and overall attack volume increased 45 percent from Q2. The Philippines also saw a spike in overall attack volume, increasing 43 percent.

Fraud and brand abuse attacks on social media accounted for 17 percent of all fraud attacks in Q3 and represents a 75 percent increase over the same time last year.

RSA recovered over 5.1 million unique compromised cards in Q3, and a total of more than 26 million since the start of 2019. Over 90 percent of compromised payment cards uncovered by RSA this year can be attributed to banks and consumers in just 15 countries.

FEATURE ARTICLE

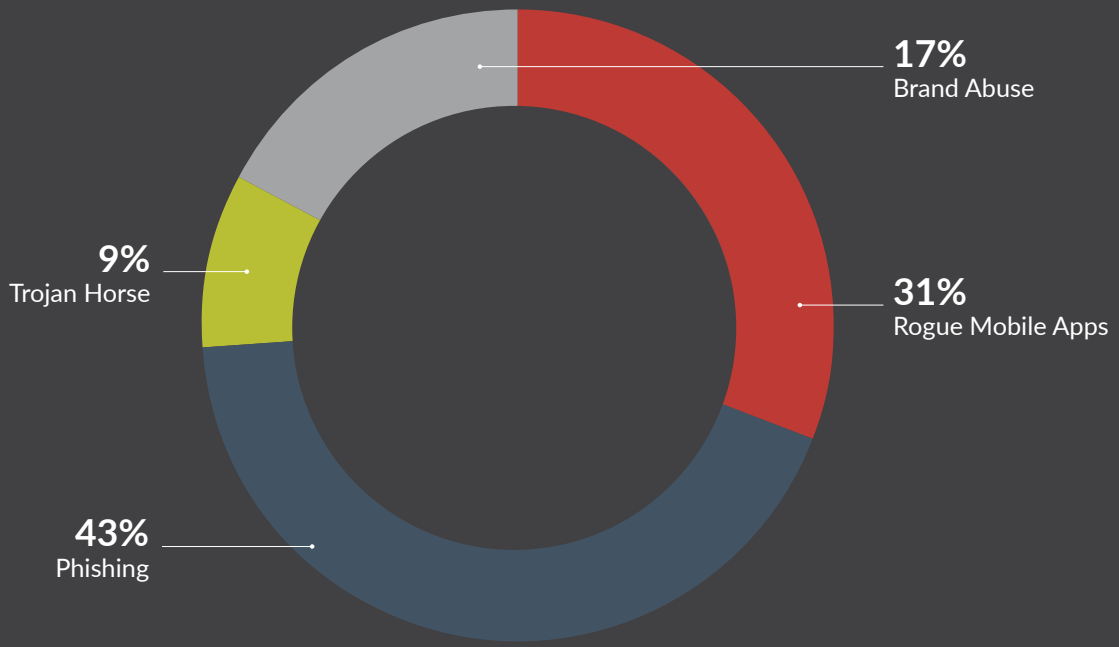
More Stolen Credit Cards Top Fraudsters' Holiday Wish List

Holiday shopping is in full swing, and during this season, it is common practice among fraudsters to start advertising their own holiday offers on the black market. These ads come in a variety of forms. In some cases, they are looking for mules to assist in performing money transfers or the reshipment of goods. Other ads offer compromised card details for sale. It is not uncommon to see card data sold in bulk as fraudsters look to offload excess inventory. In this article, we explore the countries most preferred by fraudsters in the carding business and what factors are fueling this dark web economy.

FRAUD ATTACK TRENDS: Q3 2019

Phishing and malware-based attacks are the most prolific online fraud tactics developed over the past decade. Phishing attacks not only enable online financial fraud but these sneaky threats also chip away at our sense of security as they get better at mimicking legitimate links, messages, accounts, individuals and sites. Automated fraud comes in the form of the various active banking Trojan horse malware families in the wild today; these malicious programs do their work quietly and often without detection until it is too late.

By tracking and reporting the volume and regional distribution of these fraud threats, RSA hopes to contribute to the ongoing work of making consumers and organizations more aware of the current state of cybercrime and fueling the conversation about combating it more effectively.



Fraud Attack Trends: Q3 2019

Fraud Attack Type Distribution

In the third quarter of 2019, RSA identified 55,484 total fraud attacks worldwide. RSA detected 23,800 phishing attacks, representing 43 percent of all fraud attacks identified and a 6 percent increase from last quarter. Fraud and brand abuse attacks on social media accounted for 17 percent of all fraud attacks in Q3 and represents a 75 percent increase over the same time last year.

FRAUD ATTACK GLOSSARY

Phishing
Cyber attacks attempting to steal personal information from unwitting end-users under false pretenses either by email, phone call (vishing) or SMS text (smishing).

Trojan Horse
Stealthy malware installed under false pretenses, attempting to steal personal user information.

Brand Abuse
Online content, such as social media, that misuses an organization's brand with the purpose of misleading users.

Mobile Application Fraud
Mobile applications using an organization's brand without permission.

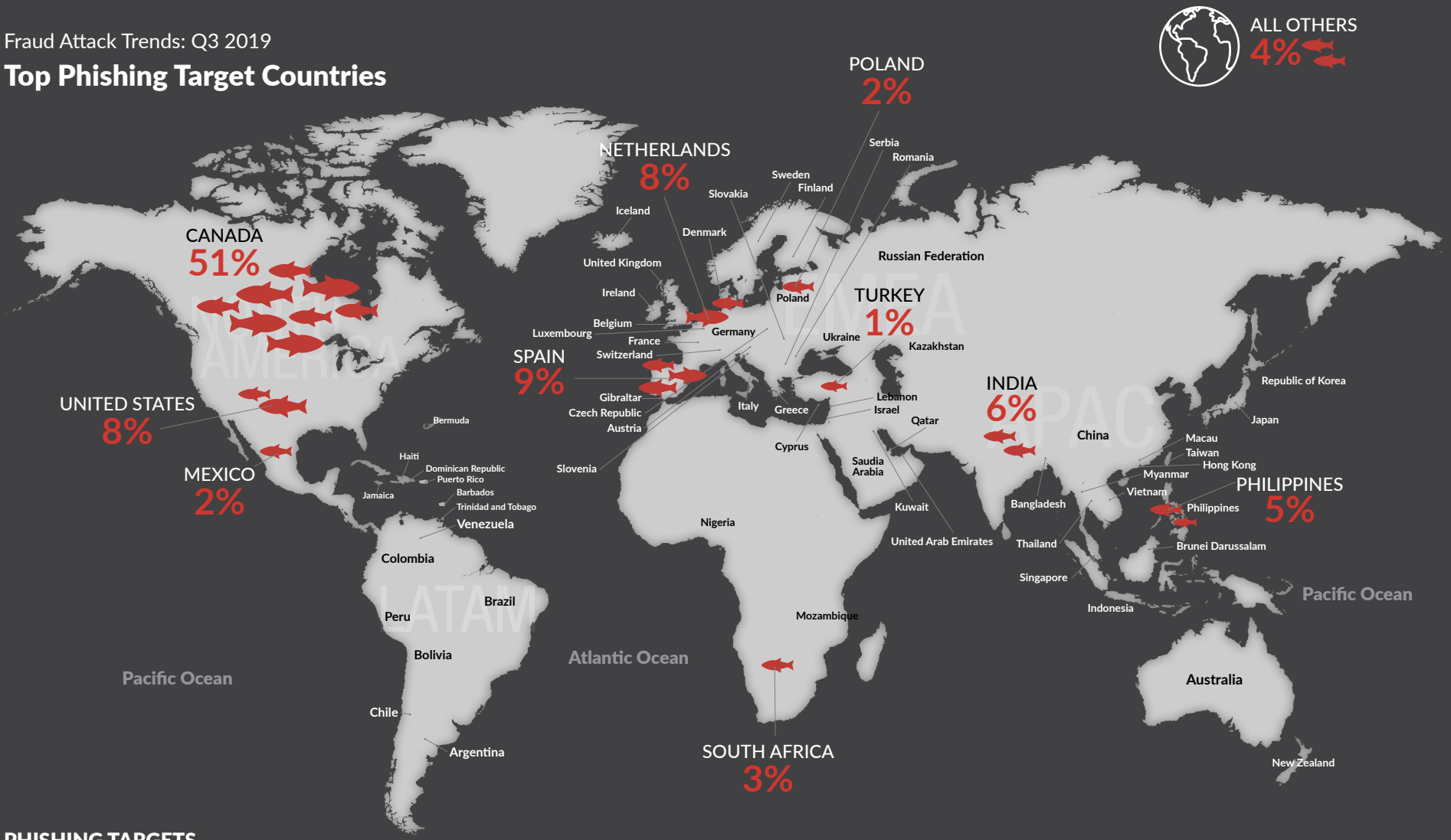
IN Q3 2019,
RSA identified over

16,900

ROGUE MOBILE APPS

Fraud Attack Trends: Q3 2019

Top Phishing Target Countries



PHISHING TARGETS

Canada, Spain and the Netherlands were the top three countries targeted by phishing, representing 68 percent of total attack volume. Poland appeared on the list replacing Turkey as a top target with 2 percent of total phishing volume in Q3.

Canada remained the top targeted country in Q3, and overall attack volume increased 45 percent from Q2. The Philippines also saw a spike in overall attack volume, increasing 43 percent. However, Spain and India saw a decrease in overall attack volume. Phishing attacks targeting Spain decreased 19 percent while attacks targeting India decreased 38 percent in Q3.

Top Phishing Hosting Countries

HOSTING COUNTRIES

1.	United States	6.	Canada
2.	Malaysia	7.	Germany
3.	Russia	8.	Australia
4.	India	9.	Hong Kong
5.	France	10.	China

PHISHING HOSTS

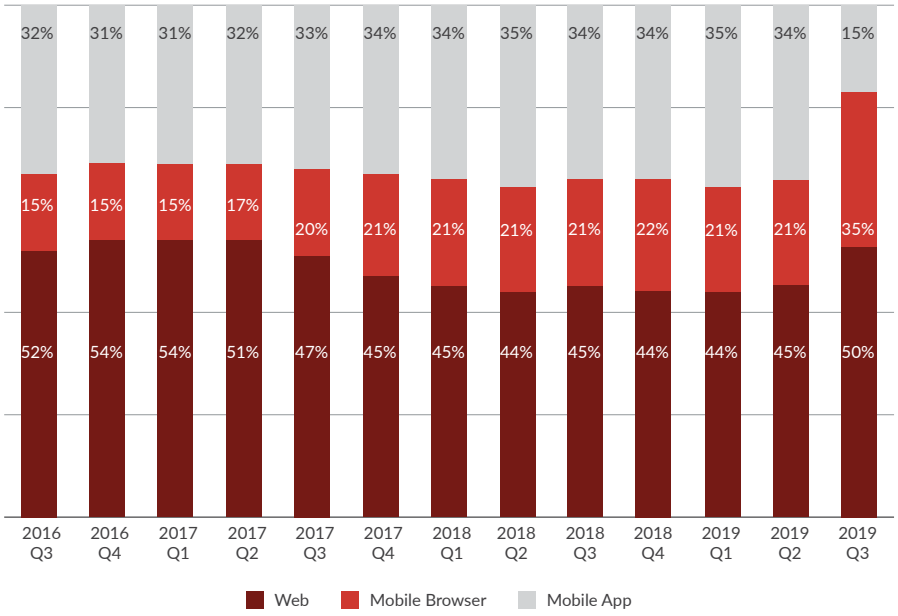
In Q3, we saw the Netherlands and United Kingdom drop from the top ten hosting country list and China and Hong Kong appeared on the list, hosting slightly more than 3 percent of overall phishing attacks. Malaysia moved to the second top hosting country with 8 percent of phishing attacks hosted there in Q3.

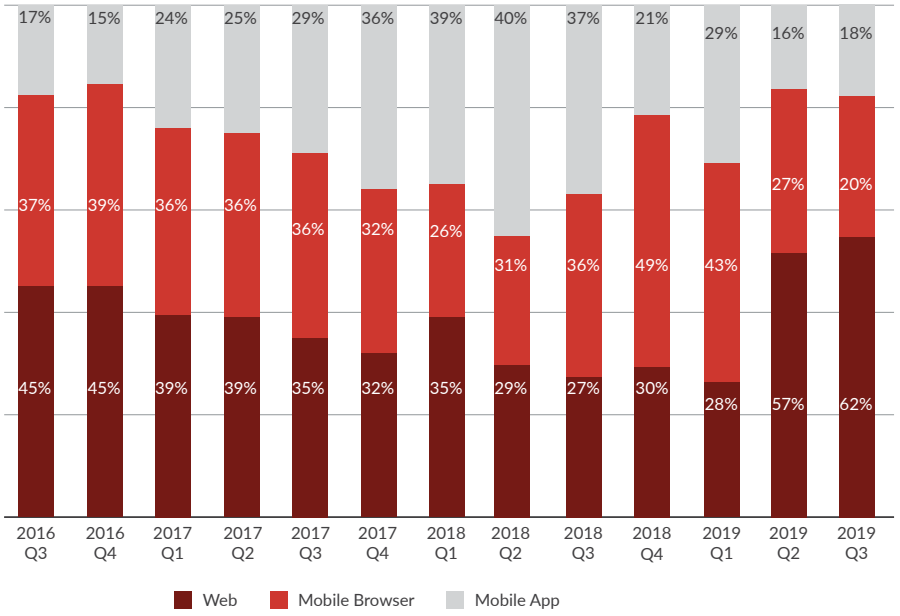
CONSUMER FRAUD TRENDS: Q3 2019

The RSA Fraud and Risk Intelligence team analyzes consumer fraud data and informs the security and risk management decisions for major organizations while serving the public interest by identifying, preventing and reducing financial cyber fraud attacks on consumers. Observing consumer fraud trends over time can support decision-makers on how to build or refine their digital risk management strategy across customer-facing deployments.

These data points are intended to broadly frame the current consumer fraud atmosphere, and identify relevant trends, by tracking broad indicators of online fraud across both financial and e-commerce focus areas.

Transaction and Fraud Transaction Distribution by Channel





Source: RSA Fraud & Risk Intelligence Service, July 2019-September 2019

TRANSACTION METHOD

In the third quarter of 2019, mobile browsers and applications accounted for 50 percent of overall transactions observed by RSA. Transaction volume in the mobile channel saw significant growth just a few years ago; however, it has remained steady and adoption has started to taper off.

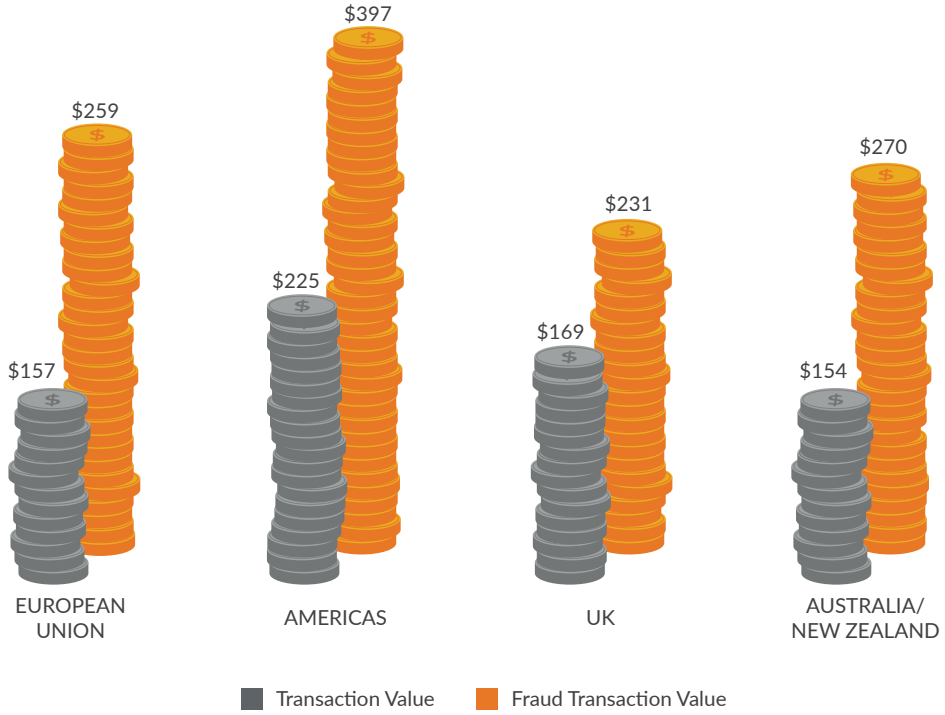
FRAUD TRANSACTION METHOD

In Q3, the shift in fraud transactions across channels continued with only 38 percent of fraud transactions originating in the mobile channel compared to the 60 – 70 percent range it has been in previous quarters. Fraud in the web channel, although declining slightly, accounted for 62 percent of fraudulent transactions.

The average value of a fraudulent payment transaction in the mobile channel was $547.

Average Credit Card Transaction and Fraud Transaction Values

(E-Commerce, by Region)



In Q3, the most drastic difference between the value of genuine and fraud transactions was observed in North America, where the average value of a fraud transaction was $397, a 27 percent increase in fraud value from last quarter. In the UK, for the last several quarters, there has been little difference in the average value of a genuine vs. fraudulent transaction as compared to other regions.

REGION	TRANSACTION VALUE	FRAUD TRANSACTION VALUE	DIFFERENCE $
European Union	$157	$259	$102
Americas	$225	$397	$172
UK	$169	$231	$62
Australia/New Zealand	$154	$270	$116

Source: RSA Fraud & Risk Intelligence Service, July 2019-September 2019

Device Age vs. Account Age

ANALYSIS

"Device Age" refers to how long the RSA Fraud Platform has "known" or "trusted" a given device (laptop, smartphone, etc.). "Account Age" refers to how long the RSA Fraud Platform has "known" or "trusted" a given account (login, etc.). This data demonstrates the importance of accurate device identification to minimize false positives and customer friction during a login or transaction event.

E-COMMERCE

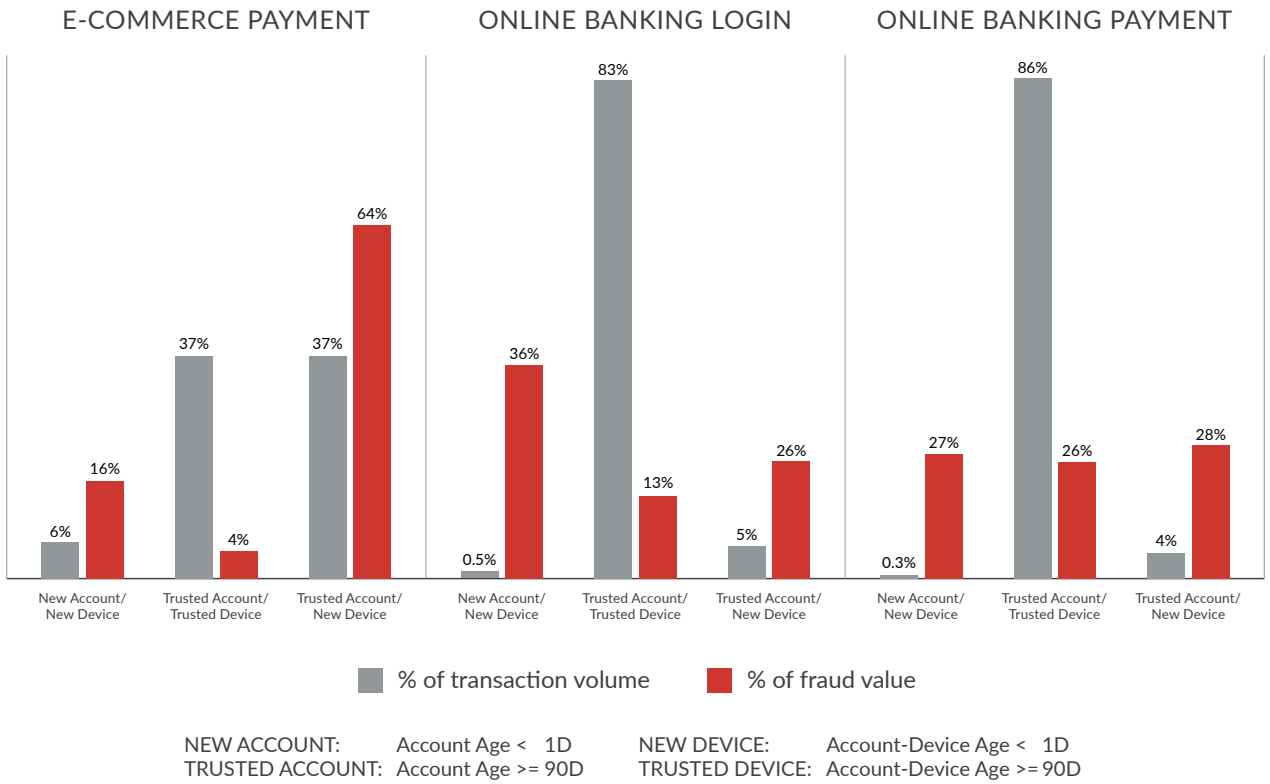
In Q3, 64 percent of fraud transaction value originated from a new device but trusted account, indicating account takeover activity continues to be a preferred and successful attack vector for cybercriminals. Sixteen percent of fraud value originated from a new account and new device, indicating the purchase of goods using stolen credit cards.

ONLINE BANKING: LOGIN

While less than 1 percent of logins were attempted from a combination of a new account and new device, this scenario accounted for 37 percent of total fraud volume observed in Q3.

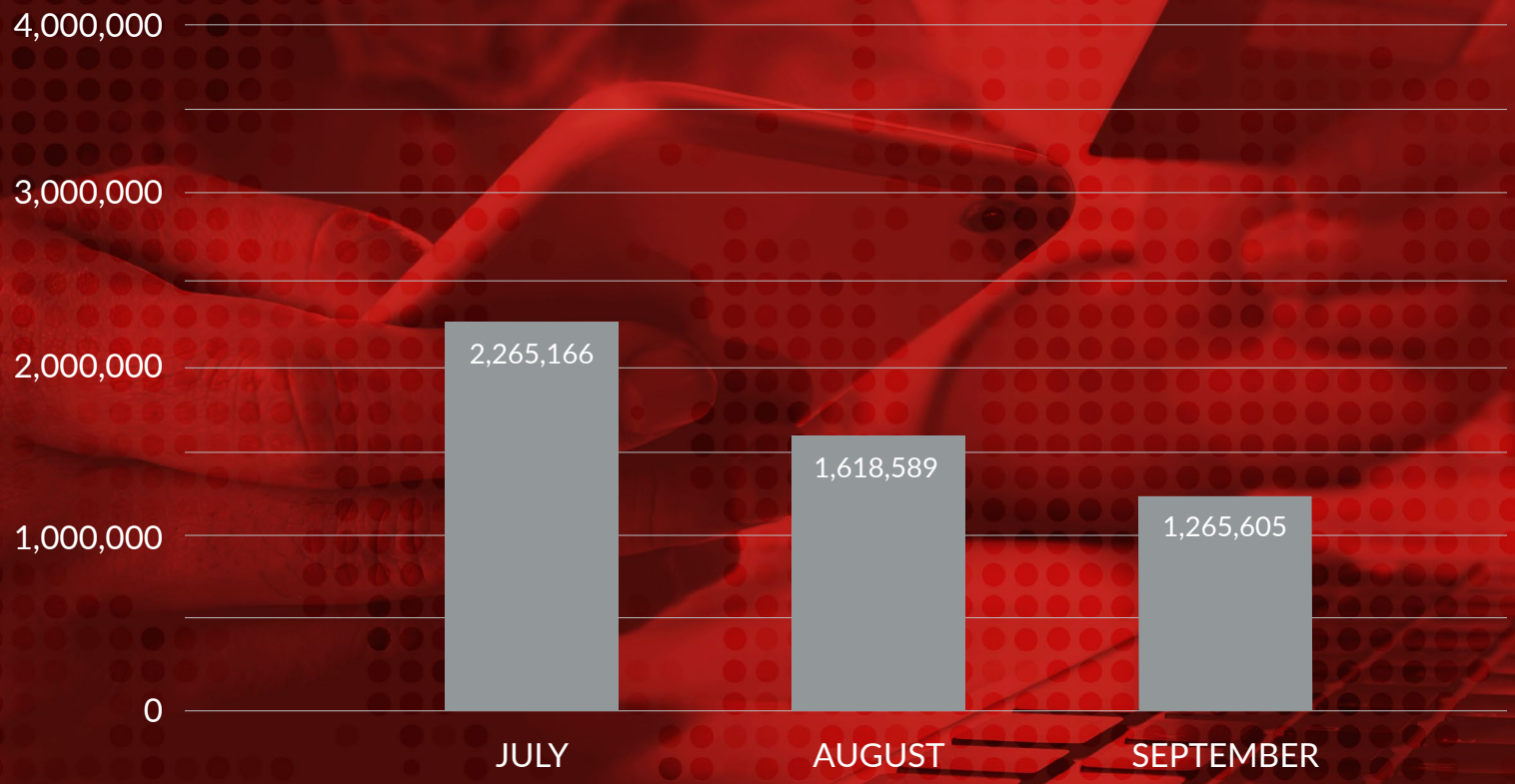
ONLINE BANKING: PAYMENT

In Q3, despite representing only 0.3 percent of total payment transactions, 27 percent of payment fraud attempts originated from a new account and new device, a significant increase from only 4 percent last quarter. This indicates a substantial increase in new account fraud where fraudsters are attempting to use compromised credentials (most likely from password breaches) to open mule accounts in order to send and receive fraudulent payments.



Source: RSA Fraud & Risk Intelligence Service, July 2019-September 2019

Compromised Credit Cards Discovered/Recovered by RSA



Source: RSA Fraud & Risk Intelligence Service, July 2019-September 2019

ANALYSIS

In Q3 2019, RSA recovered over 5.1 million unique compromised cards and card previews, a 24 percent decrease in cards recovered in the previous quarter. Despite the quarter-over-quarter decrease, since the start of 2019, RSA has uncovered more than 26 million unique compromised payment cards and card previews from reliable online fraud stores, social media and other sources. This represents a 23 percent increase from 2018. Over 90 percent of the compromised payment cards uncovered by RSA can be attributed to banks and consumers in just 15 countries.

FEATURE ARTICLE

More Stolen Credit Cards Top Fraudsters' Holiday Wish List

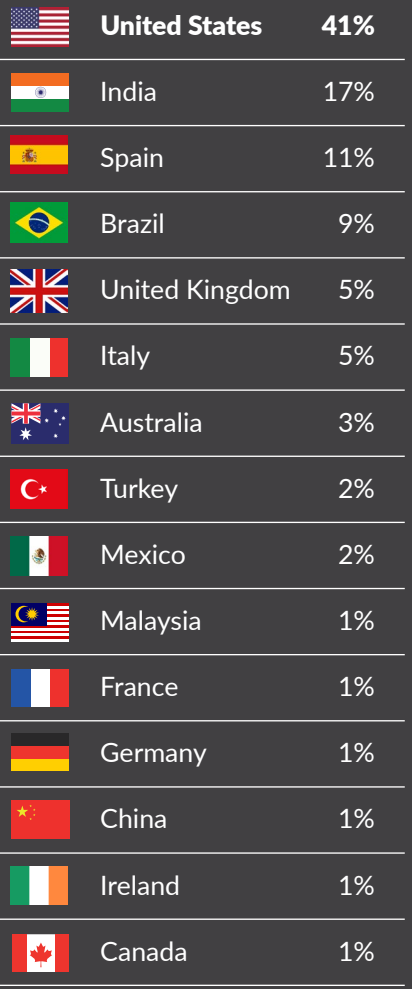
E-commerce continues to take a bigger bite out of holiday shopping sales, and this year is no exception. In fact, according to a study by Deloitte, 59% of holiday shopping will be done online with expected sales in the range of $144 million to $149 billion. Fraudsters are well aware of this and have been preparing all year in a number of ways.

Starting well in advance of the Black Friday sale day that kicks off the holiday shopping season for so many consumers, it is common practice among fraudsters to start advertising their own Black Friday sales and offers in the black market. These ads come in a variety of forms. In some cases, they are looking for mules to assist in performing money transfers or the reshipment of goods. Other ads offer compromised card details for sale. It is not uncommon to see card data sold in bulk as fraudsters look to offload excess inventory. Card details are sold across regions and come in the form of both CVVs (captured online payment card details that are mostly obtained through phishing and malware) and dumps (magnetic stripe/track details that are obtained via ATM or PoS skimming and used for cloning physical cards).

Below is an example of just one of many ads posted by a fraudster in an ICQ fraud group. The price per compromised card depends on the region where the stolen card originates.

Consumers would do well to monitor their credit card and bank statements more frequently for fraudulent activity at this time of year, looking specifically for purchases they did not make.

PERCENTAGE OF PAYMENT CARDS FOR SALE



United States	**41%**
India	17%
Spain	11%
Brazil	9%
United Kingdom	5%
Italy	5%
Australia	3%
Turkey	2%
Mexico	2%
Malaysia	1%
France	1%
Germany	1%
China	1%
Ireland	1%
Canada	1%

ICQ chat rooms are not the only places that fraudsters are advertising their illicit wares. They continue to expand their advertising across social media as well. A comprehensive study of this phenomenon by RSA® showed that more than 50% of fraudulent activity occurring on social media was attributed directly to carding and the sale of compromised cards.

Since the start of 2019, RSA has uncovered more than 26 million unique compromised payment cards and card previews from reliable online fraud stores and other sources. This is a 23% increase from 2018. Other large caches of stolen payment cards have also recently been reported including the infamous BriansClub which was itself hacked and its database of stolen card information leaked to cybersecurity blogger Brian Krebs.

Based on the compromised payment cards recovered by RSA from online credit card stores during the first half of 2019, an in-depth analysis of the data shows that 92% of all compromised payment cards for sale on the black market can be attributed to just 15 countries. Among those countries, 88% of all compromised cards can be attributed to only six countries. The breakdown of compromised payment cards among the top 15 countries follows (See chart at left).

Overall, card demand per country stems from a variety of factors. An obvious one, for example, is the number of people within a specific region who are falling for phishing or malware attacks which fuel the card economy. A more practical one is the number of options available to the fraudster for cashing out the card such as the ability to link the card to various payment services or commit e-commerce fraud. In other words, how easy is it to monetize the card?

During this year's holiday shopping season, it is important for consumers to be extra vigilant. Consumers should be wary of phishing emails or text messages purporting to be from their bank or card issuer. A recent warning from the Cybersecurity and Infrastructure Security Agency (CISA) noted that because consumers are likely to be spending more on high-ticket items, they might expect to receive an alert asking to confirm a suspicious transaction. Criminals know this and will take advantage of consumers having their guard down and send messages attempting to redirect them to a phishing site or to download malware.

Consumers would also do well to monitor their credit card and bank statements more frequently for fraudulent activity at this time of year, looking specifically for purchases they did not make. E-commerce fraud is particularly prevalent now, as fraudsters know that merchants and card issuers might relax their standard security protocols during the holiday shopping frenzy in order to increase transaction volume and avoid interruptions to the customer experience.

Black Friday was originally a phrase used to describe the disorder and traffic congestion in shopping areas the day after Thanksgiving. Retailers did not like the negative connotation and tried to spin it into a positive by using the name as an indicator of profitability due to the increased shopping traffic during the holidays. As retailers go into the black (profit) and consumers go into the red (debt), let's make sure it is at our own behest and not the result of a fraudster.

DIGITAL RISK IS EVERYONE'S BUSINESS
HELPING YOU MANAGE IT IS OURS

RSA offers business-driven security solutions that provide organizations with a unified approach to managing digital risk that hinges on integrated visibility, automated insights and coordinated actions. RSA solutions are designed to effectively detect and respond to advanced attacks; manage user access control; and reduce business risk, fraud and cybercrime. RSA protects millions of users around the world and helps more than 90 percent of the Fortune 500 companies thrive and continuously adapt to transformational change.

Find out how to thrive in a dynamic, high-risk digital world at rsa.com

RSA®