RSAConference2020

San Francisco | February 24 – 28 | Moscone Center

HUMAN ELEMENT

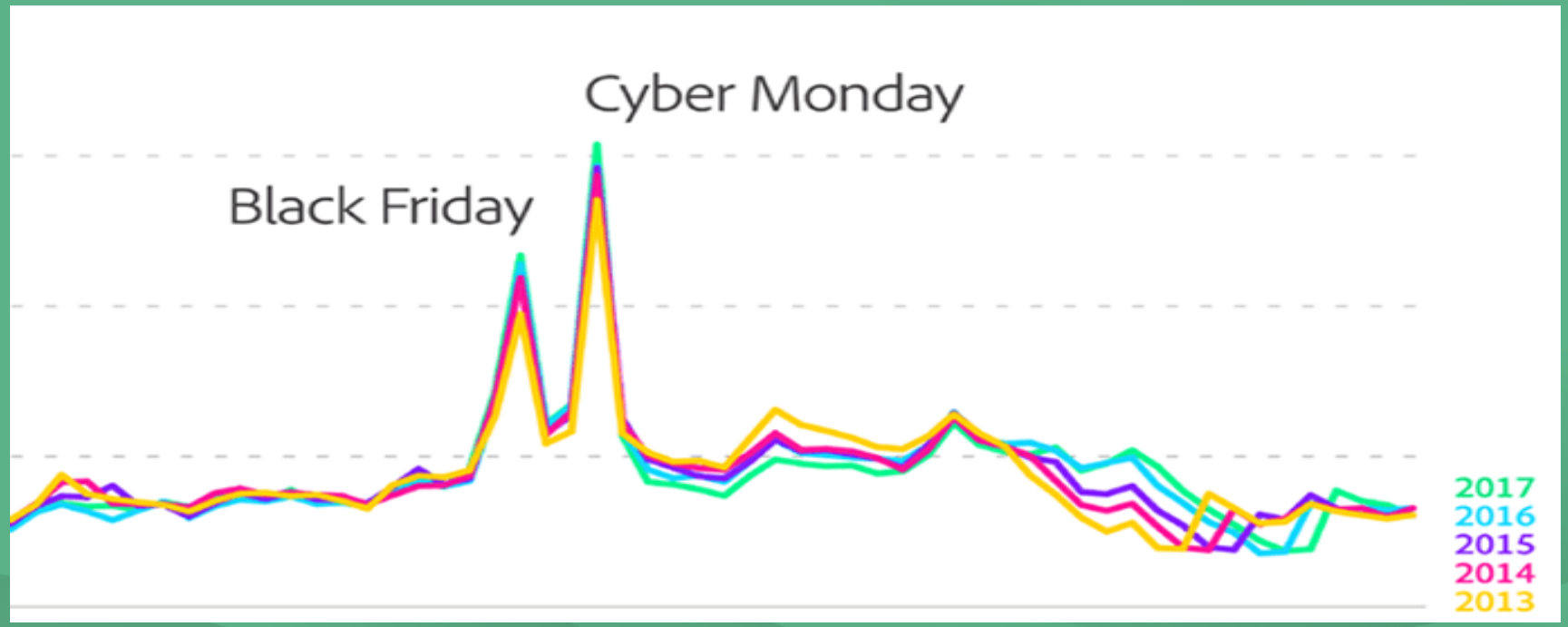
SESSION ID: **AFD-F03**

“We’re Trending!!” When Traffic Is Spiking, How Do You Know It’s Legit?

Gilit Saporta

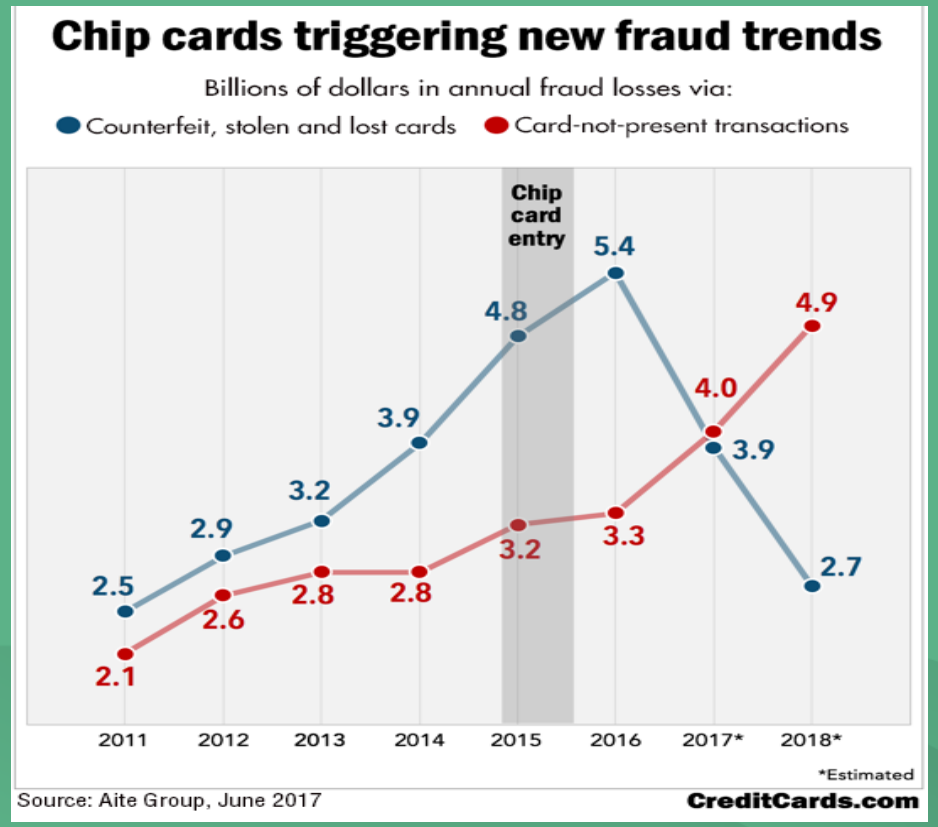
Head of Fraud Intelligence
Simplex.com
Gilits@Simplex.com / Gilit@RiskSalon.org

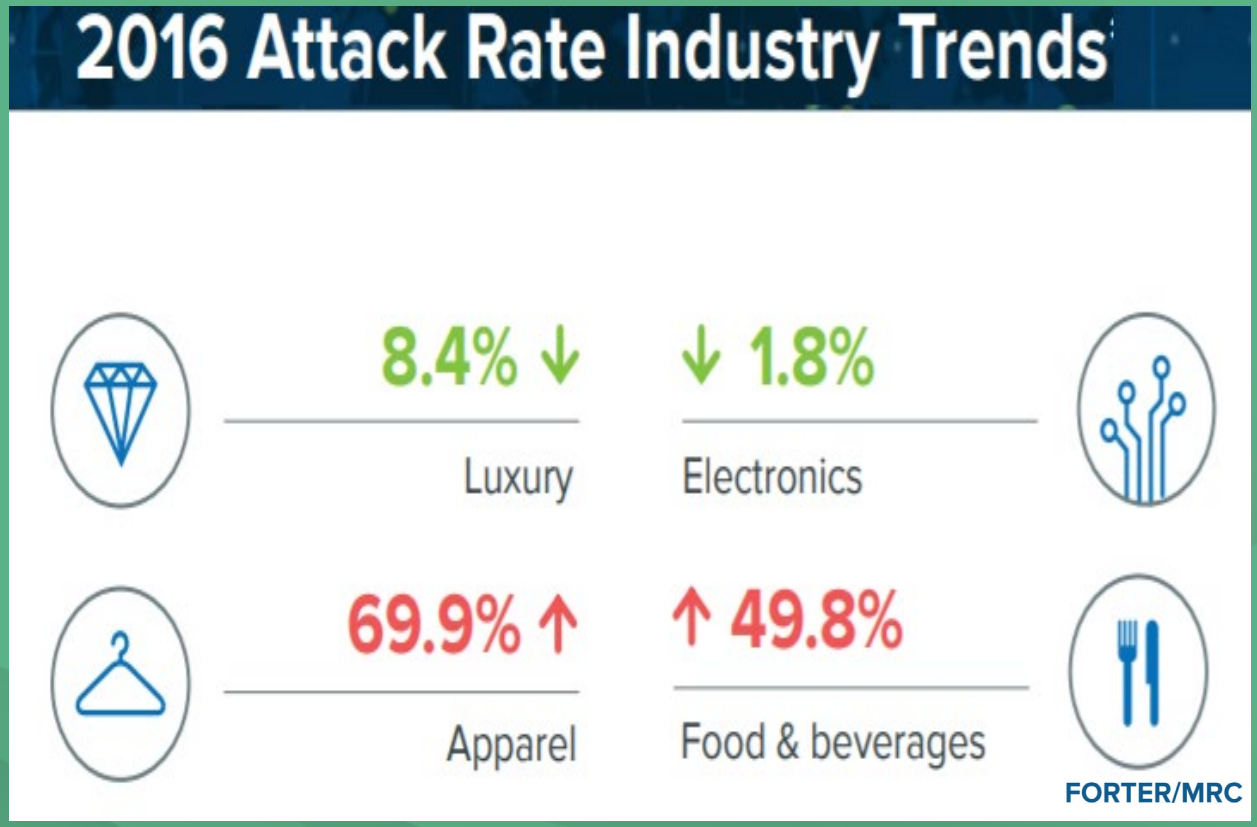
RSAConference2020



Some Trends and Spikes in Sales are Seasonal, While Others May Come as a Pleasant(?) Surprise

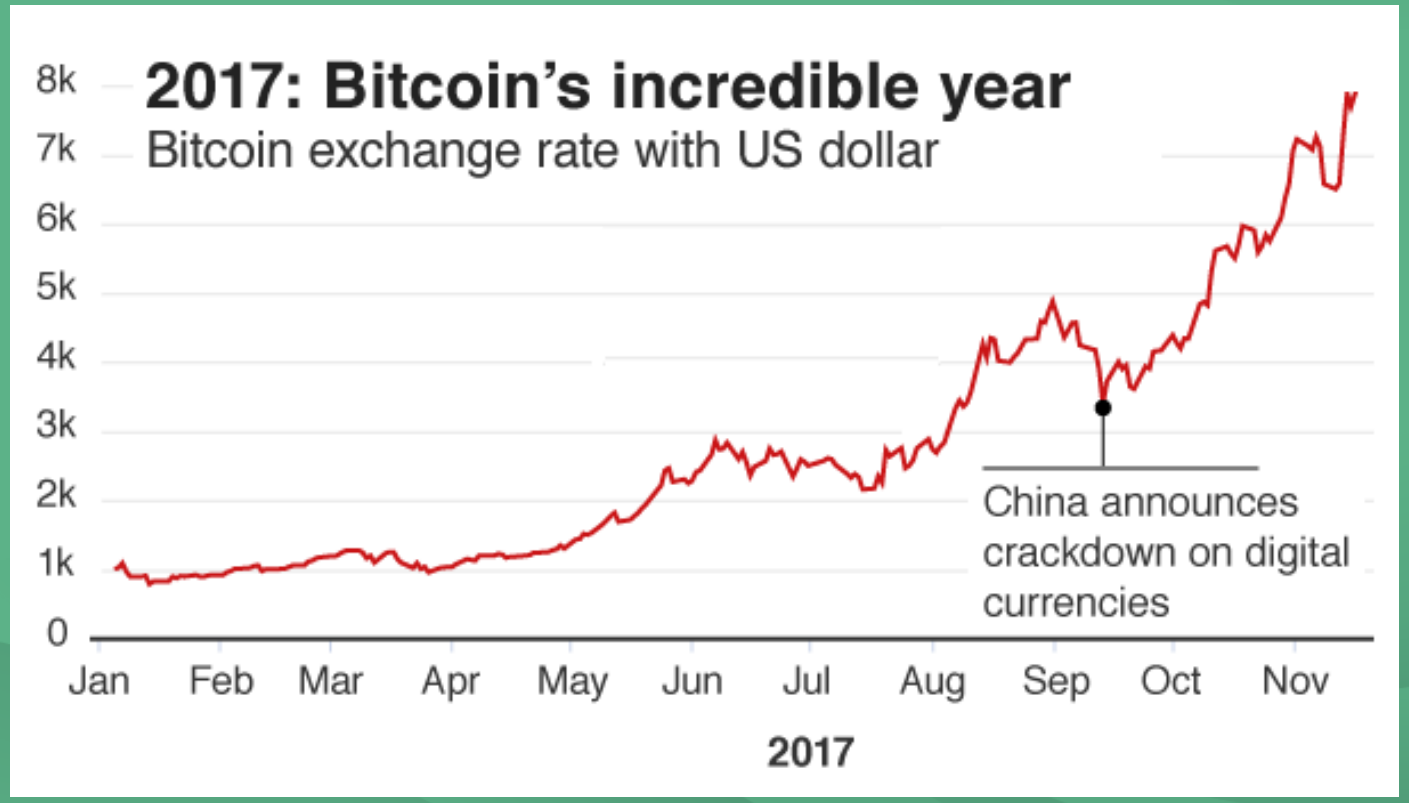
RSAConference2020





If you were an eCommerce retailer in 2016, you felt it…

RSAConference2020



If you were a Cryptocurrency exchange in 2017, you felt it…

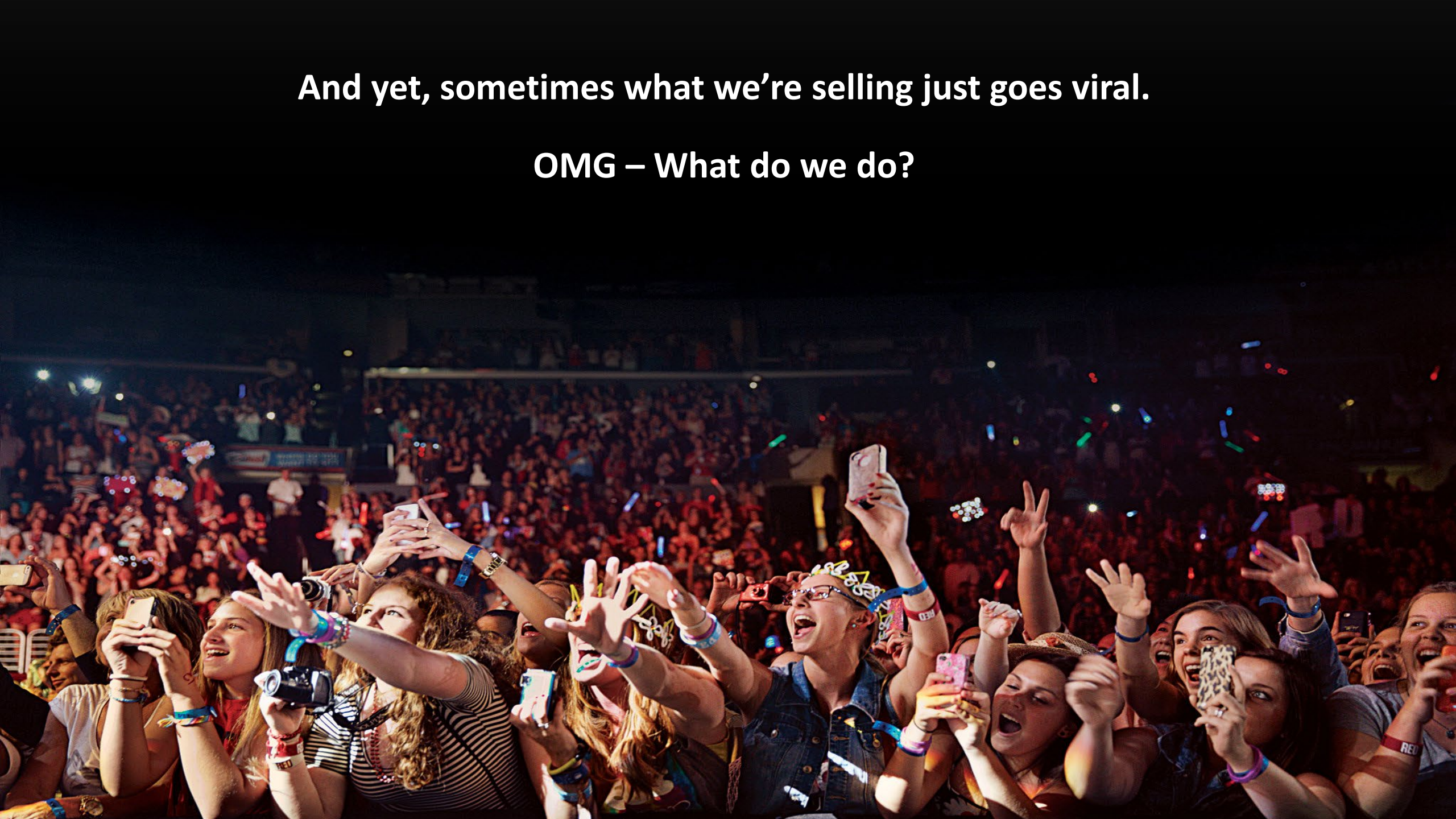
Mitigating the Unexpected: How To Analyze Spikes?

- For fraud fighters, there's no such thing as a pleasant surprise.
- If Sales are suddenly spiking, we **must** find out **why**.
  - Tip: don't be surprised!

  Learn about new products, flows, markets & regulations in advance.

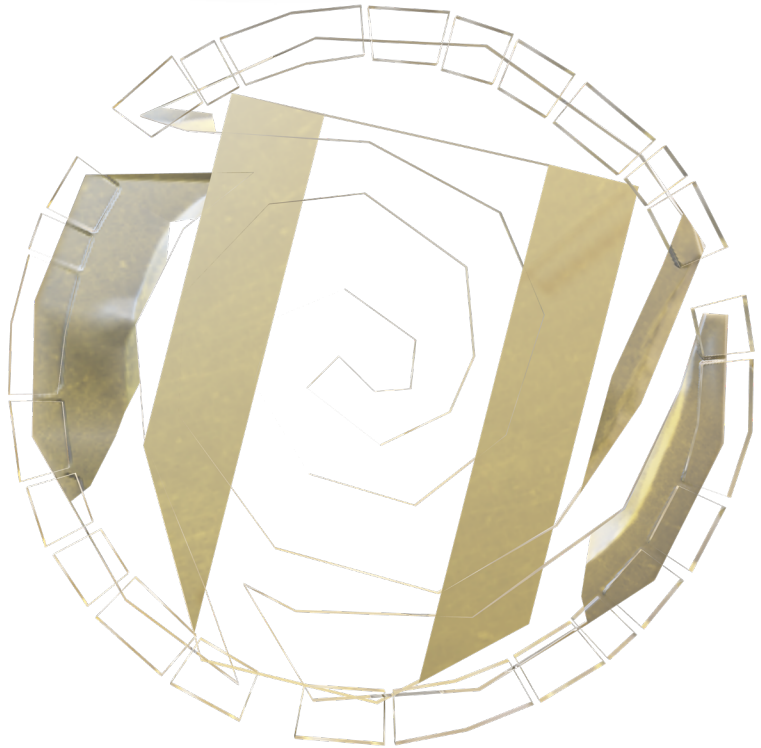
And yet, sometimes what we're selling just goes viral.

OMG – What do we do?



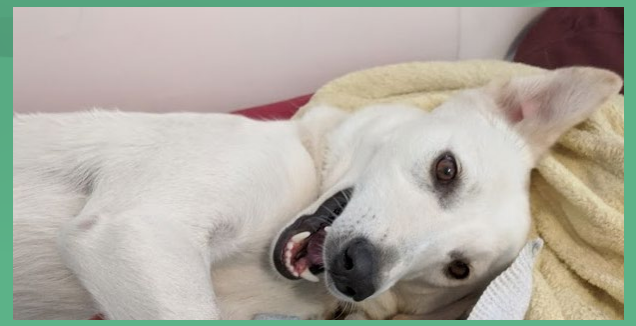
Analyze “Hot” Items by Looking at Both Sides of The Coin

- For your legit traffic:
  - Retrain models to expect high velocity
  - Raise limits for returning buyers
  - Accept that legit users act out during spikes



- For your fraudsters:
  - Proactive manual review of new flows
  - Shields up against **phishing** schemes!

RSAConference2020



PHISHING 101:
Fraudster promises to sell you a puppy, then uses your details to buy Bitcoin

PHISHING 201:
Fraudsters promises to sell you Bitcoin, takes you through Simplex verifications flows AND saves your details to buy more Bitcoin

How to Spot Social Engineering in Crypto Fraud

2019-02-20	208.5	Toril S[redacted]pstad	492557 *6436	DNBNOR	RND:
2019-02-20	2283.08	Toril S[redacted]pstad	492557 *6436	DNBNOR	4J3Aqw
2019-03-02	1303.13	Toril S[redacted]pstad	492557 *6436	DNBNOR	4J3Aqw
2019-03-02	2085	Toril S[redacted]pstad	492557 *6436	DNBNOR	4J3Aqw
2019-03-07	208.5	toril [redacted]pstad	492557 *6436	DNBNOR	RND:
2019-03-07	208.5	COINBASE LTD	454313 *2620	NATIONWIDE BUILDING SOCIETY	RND:
2019-03-11	208.5	coinbaswe is	454638 *6557	HSBC BANK PLC	RND:

How to Spot Social Engineering in Crypto Fraud

2019-02-20	208.5	Toril S[redacted]pstad	492557 *6436	DNBNOR	RND:
2019-02-20	2283.08	[redacted]pstad	492557 *6436	DNBNOR	4J3Aqw
2019-03-02	1303.13	[redacted]pstad	492557 *6436	DNBNOR	4J3Aqw
2019-03-02	2085	Toril S[redacted]pstad	492557 *6436	DNBNOR	4J3Aqw
		toril [redacted]pstad	492557 *6436	DNBNOR	RND:
2019-03-07	208.5	COINBASE LTD	454313 *2620	NATIONWIDE BUILDING SOCIETY	RND:
2019-03-11	208.5	coinbaswe is	454638 *6557	HSBC BANK PLC	RND:

$ value increase

Inconsistent spelling

CC issued in UK for a customer in Norway

Phishing, Smurfing, Social Engineering

2019-02-20	208.5	Toril S [redacted] pstad	492557 *6436	DNBNOR	RND:
2019-02-20	2283.08	Toril S [redacted] pstad	492557 *6436	DNBNOR	4J3Aqw
2019-03-02	1303.13	Toril S [redacted] pstad	492557 *6436	DNBNOR	4J3Aqw
2019-03-02	2085	Toril S [redacted] pstad	492557 *6436	DNBNOR	4J3Aqw
2019-03-07	208.5	toril [redacted] pstad	492557 *6436	DNBNOR	RND:
2019-03-07	208.5	COINBASE LTD	454313 *2620	NATIONWIDE BUILDING SOCIETY	RND:
2019-03-11	208.5	coinbaswe is	454638 *6557	HSBC BANK PLC	RND:

Victim buys crypto via phishing website, Fraudster records card

Fraudster makes more payments with victim's card

Victim buys again, this time fraudster gains access to her PC

Fraudster uses victim's device & account to monetize cards

simplex

RSAConference2020

It’s not just Bitcoin!

Phishing scams are threatening all Digital Goods

iTunes and Taxes SCAM

"…I received a call from a person who claimed to be an SSA employee.
He said that my SSN and name were associated with a murder & money-laundering scheme…
Said that that my SSN would be suspended.
To clear my name, I would be issued a new social security number… my cash assets must be transferred to a government protected account, by purchasing cash gift cards with bitcoin and using them to establish a credit line in support of the "new" social security number.
I believed him…."


The Full Impact of Social Engineering
Might Be Revealed Months or even Years After the Attack

A Word For Customer Care & User Awareness

- Fraud victims often feel empowered when they learn how to say “no”

to: "Simplex Support" <support@simplexcc.com>

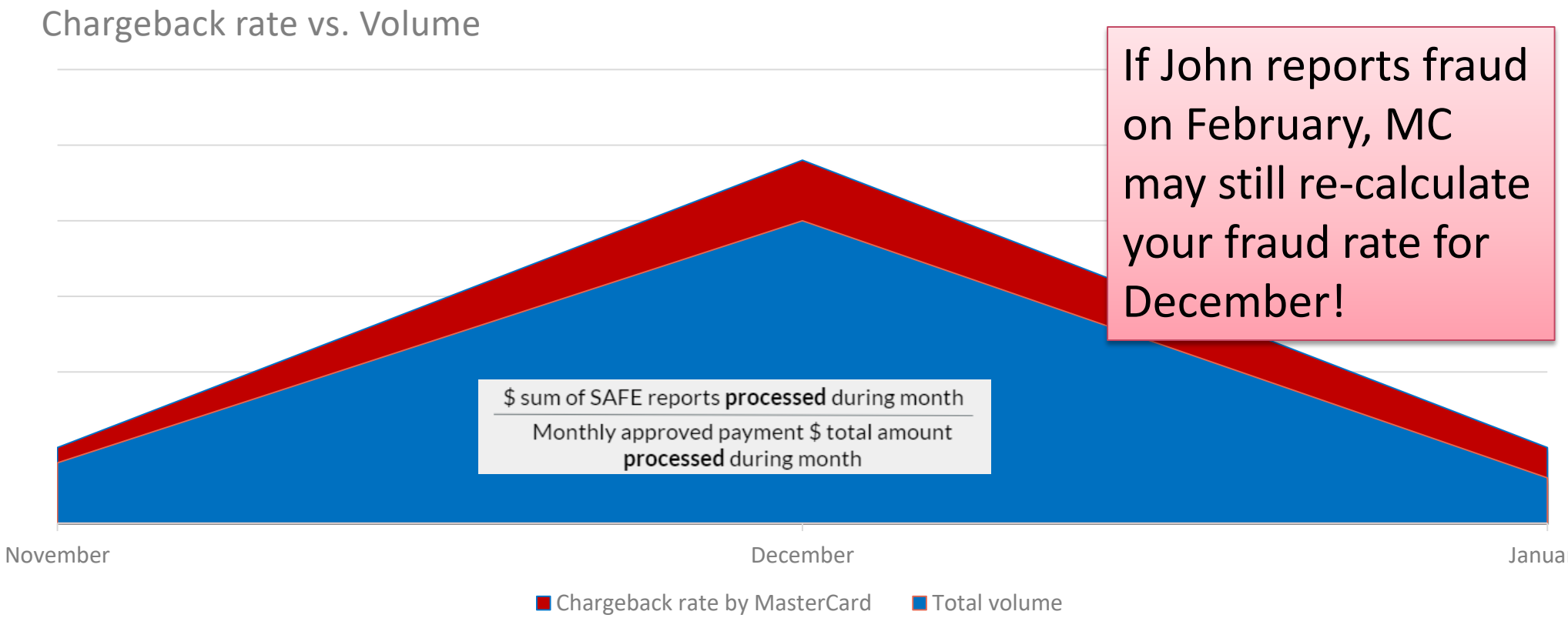
Dear Justine and members of the Simplex Team,

Thank you for your investigation and assurance;

I still remain shocked by my gullibility and I need to reflect deeply on how I could have been so entangled in such a scam.

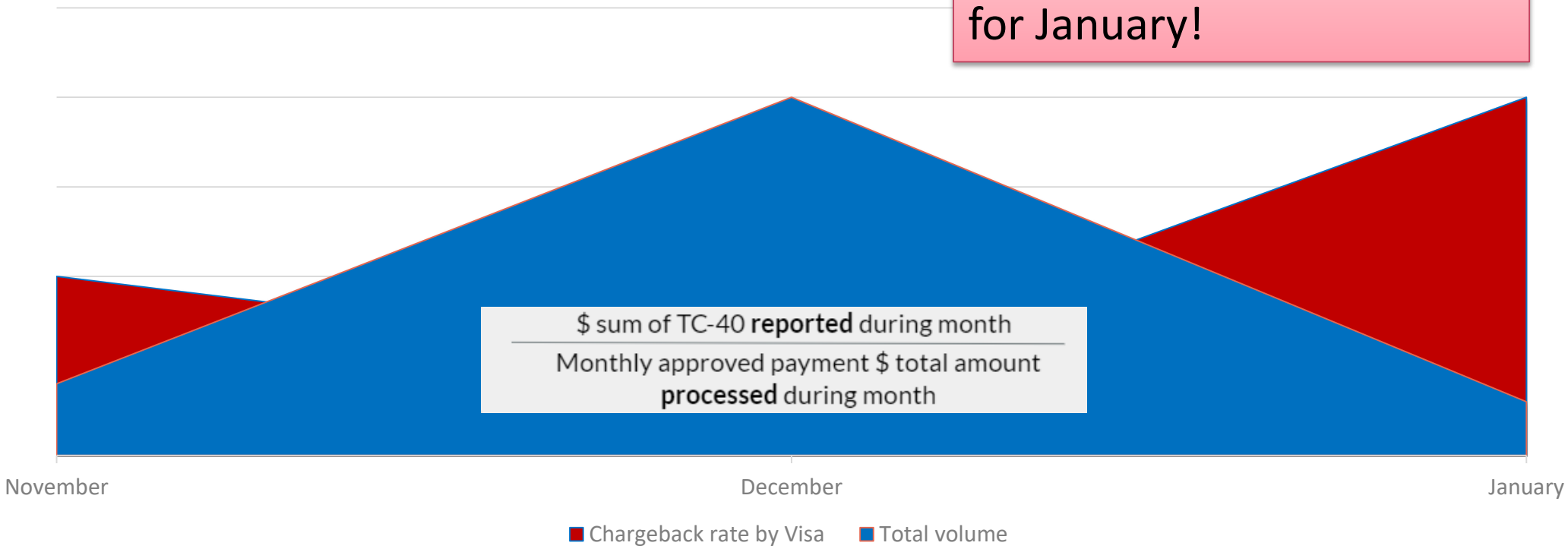
I realize that you are not responsible for this fraud.

MasterCard is Extra Sensitive to Social Engineering, Because Victims Report Them Late!



Visa is Sensitive to all Fraud Spikes, But Only for ~1 Month

If on January, John reports the fraud of December, Visa will up your fraud rate for January!



RSAConference2020

PAUSE FOR QUESTIONS,
then
TIME TO PRACTICE!

Is the next slide a good spike or a bad spike?

#1 - Good Spike or Bad Spike?

- November 2019 - Greek **airline** shows 12% uptick in traffic
  - Average daily heatmap of IP geolocation for the spike:

Good Spike or Bad Spike?

- November 2019 - Greek **airline** shows 12% uptick in traffic
  - Heatmap of IP geolocation for the spike:
  - Heatmap of **CC-issuer-bin** geolocation for the spike:
  - Destination:

BAD SPIKE!

- Most plausible story is a fraudster who's selling tickets for cash to refugees, then paying with stolen Scandinavian CCs online

#2 - Good Spike or Bad Spike?

- July 2019 – Bitcoin exchange shows a 21% spike from China IPs
- Top 10 CC bins: Sri-Lanka, US, Vietnam, Germany, Sweden, Hong Kong, Malta, Gibraltar, Luxemburg, Cyprus

Good Spike or Bad Spike?

- July 2019 – Bitcoin exchange shows a 21% spike from China IPs
- Top 5 CC bins: Sri-Lanka, US, Vietnam, Germany, Sweden

Good Spike or Bad Spike?

Investopedia

Is Bitcoin Banned in China?

By SHOBHIT SETH | Updated Jun 25, 2019

Earlier this month, the People's Bank of China (PBOC) which is the central regulatory authority that regulates financial institutions and drafts the monetary policy of the country, issued a statement that "it would block access to all domestic and foreign cryptocurrency exchanges and ICO websites."

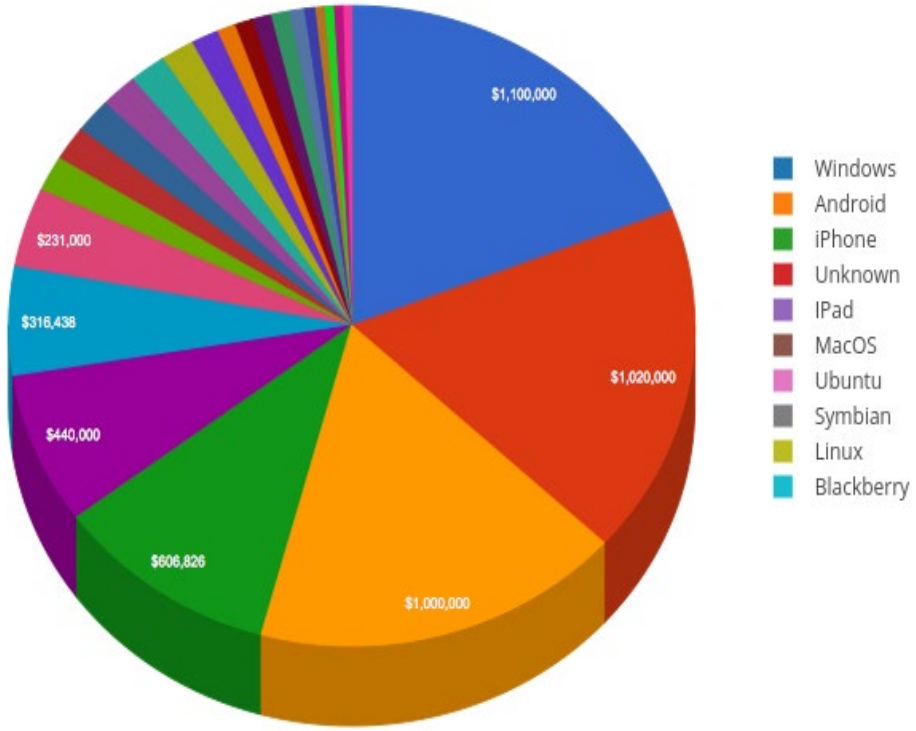
As per the news, China aims to clamp down on "all cryptocurrency trading with a ban on foreign exchanges."

Good Spike (sort of)

- The most plausible story is that China citizens are using foreign payment methods to circumvent Chinese regulation
- No chargeback risk, but clear business/legal risk

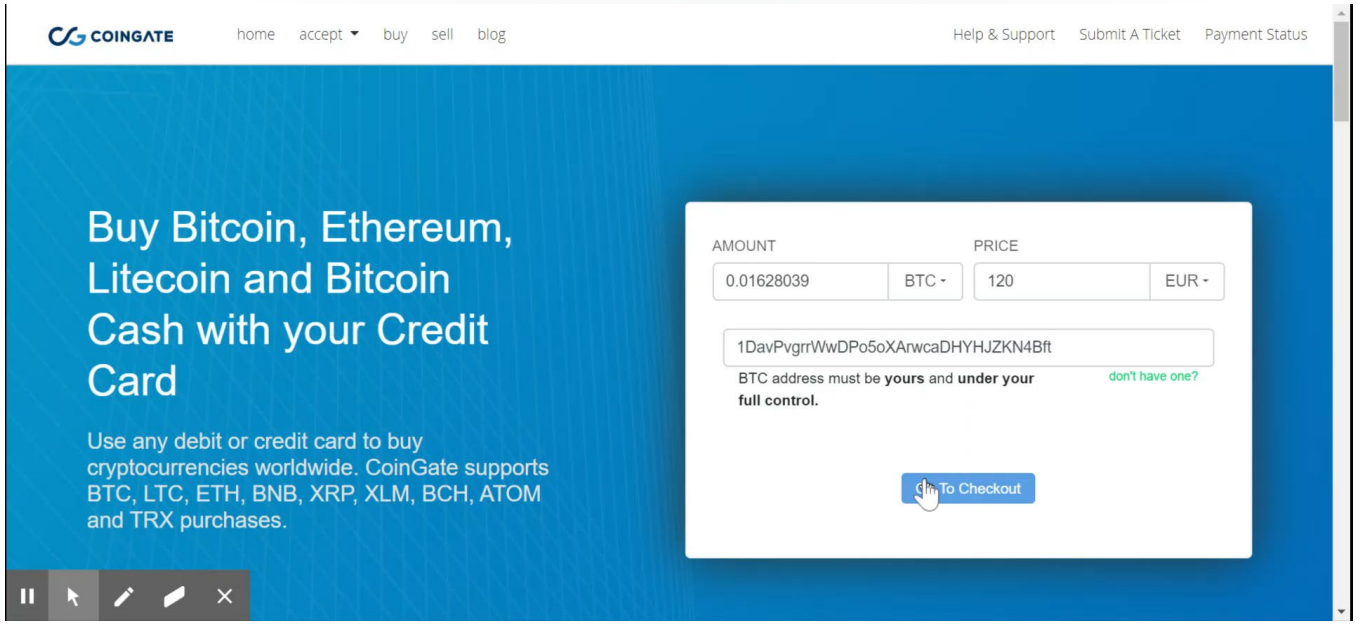
#3 Good Spike or Bad Spike?

- Over 1,000 payments coming in on a single week from Lithuania
- $ increase over 500% (for this country)
- Extra-diverse mix of devices and OS



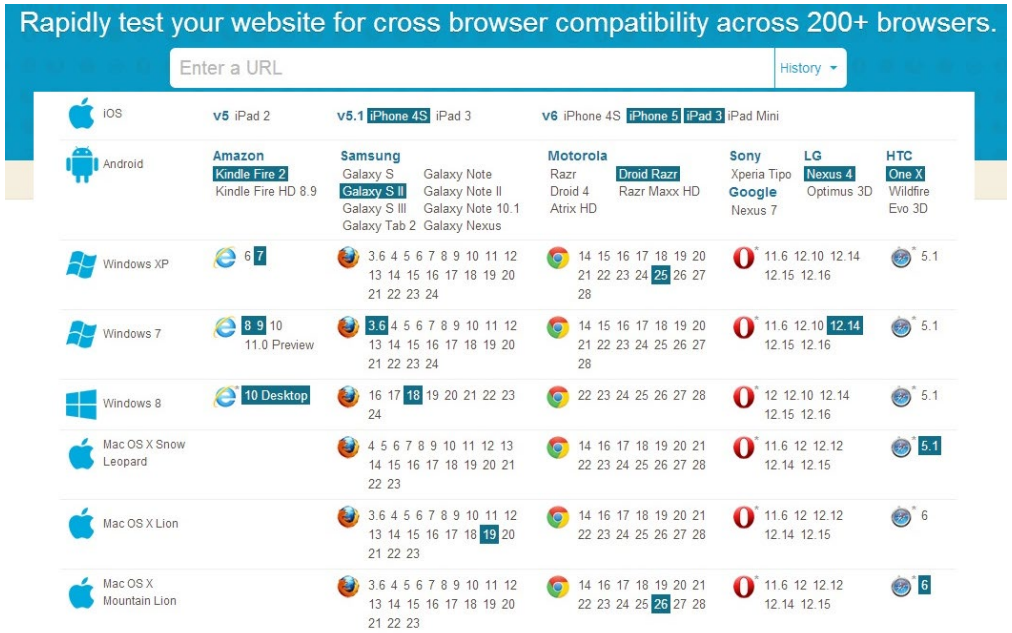
Good Spike or Bad Spike?

- Bogus registration
- Lost of fake credentials



Good Spike or Bad Spike? Not a Spike

- Obviously, dev testing the system, with impressive volumes
- This “fake spike” is a good dry run for DDOS attacks



RSAConference2020

Recap and what to take home with you

Apply What You Have Learned Today

- Next week you should:
  - Check your roadmap to try and predict this year's sales and fraud spikes
  - Proactively sample and review fraud cases from sales spikes. Are they phishy?
- In the first three months following this presentation you should:
  - Prepare a "spike-control" plan, including model training for high velocity
  - Consider raising end-user awareness to phishing schemes in your industry
- Within six months you should:
  - Execute your plan and test it on your next seasonal/occasional spike
  - Monitor and expect lower fraud rates during your next sales spike

Questions please
* just not about the future of crypto ;-)
**just kidding, ask me anything

RSAConference2020

San Francisco | February 24 – 28 | Moscone Center

HUMAN ELEMENT

SESSION ID: **AFD-F03**

THANK YOU

Gilit Saporta

Head of Fraud Intelligence
Simplex.com
Gilits@Simplex.com / Gilit@RiskSalon.org