





## Agenda



- Global Compromise Trends
- eCommerce Threat Landscape
- Tactics and Techniques used by Hackers
- What Visa is Doing
- Resources for Merchants
- Questions



# Compromise Trends



## Global Compromise Trends

The Paradigmatic Shift Explained

#### **Shifting Breach Types**

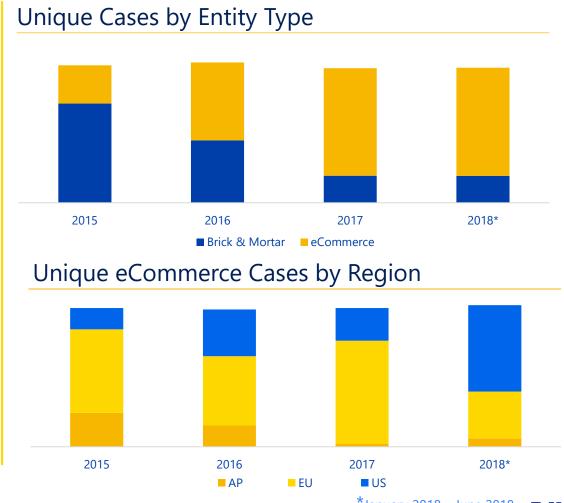
- Decrease in events involving magnetic stripe data
- Increase in eCommerce compromises
- Proliferation of third-party breaches

#### **Criminals Moving Beyond Merchants**

- Pursuing data aggregators
- Increasing focus on eCommerce service providers
- Targeting Integrators Resellers
- Penetrating financial institutions

#### **Sharpening Focus on Evolving Trends**

- Curtailing network intrusions e.g. eCommerce
- Detecting ATM cash-outs
- Minimizing account testing



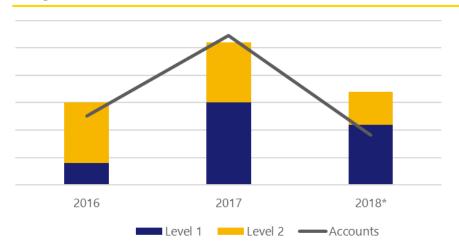


## Global Breaches Summary: Q2 2018

#### Global Breaches by Level

	2015	2016	2017	2018*
Level 1	<1%	<1%	2%	4%
Level 2	<1%	1%	1%	2%
Level 3	4%	13%	15%	28%
Level 4	76%	57%	38%	60%
Service Provider**	2%	2%	4%	6%
Europe***	17%	27%	39%	-
Total	100%	100%	100%	100%

#### Large Merchant Breaches



#### Service Provider Breaches





<sup>\*</sup> Available for 1 January 2018 – 30 June 2018.

<sup>\*\*</sup> Service Provider category includes all agents.

<sup>\*\*\*</sup> As of 1 January 2018, cases in Europe will be combined with ROW categories.

# The Threat Landscape



## An Overview of Website Add-ons and Scripts

#### What are add-ons and scripts?

Website add-ons and scripts are pieces of code that can be added to a webpage and are executed in the user's web browser.







# What role do add-ons and scripts serve?



Website add-ons and scripts provide expanded capabilities to websites. Code can be added that gathers analytical data, integrate with social media or other services.

#### What risks do website plugins and scripts pose?

Criminals are targeting third-party vendors that may be outside of the payments ecosystem – but their services can bring them directly into merchant eCommerce environments with little vetting and easy plugin capabilities.

If the hackers can breach a third-party provider of website plugins or scripts, they may be able to modify the legitimate code to steal data from 1,000s of eCommerce merchants using the service

A report by <u>PYMNTS.com</u> cited that around 85% of all call center interactions will not require a human employee by 2020 (i.e. Chatbot)

Merchants should be continually aware and up-to-date on the risks of potential exploitation. They should adopt anti-fraud and security measures that secure their clients' payment card data.

Recent agent investigations highlight the importance of securing the vendor ecosystem as well a merchant's own eCommerce environment



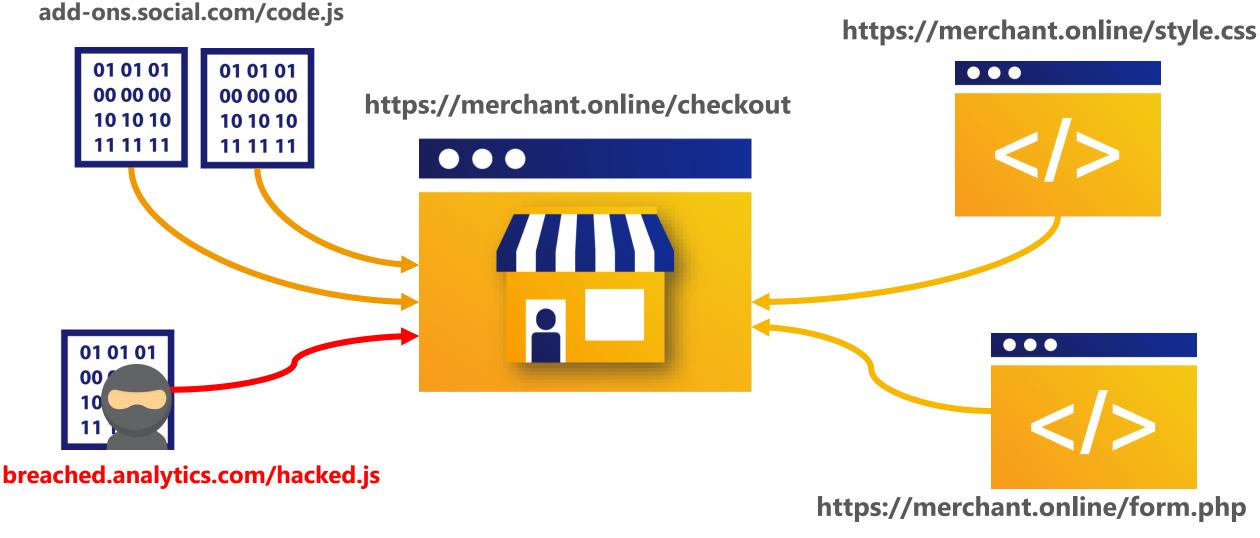
## What is ECommerce malware?

- Acts as an online payment data skimmer
- Lucrative endeavor for criminals
- Malware infections are unsophisticated, hidden in plain sight, and persistent
- Significant contributor to global fraud in CNP space

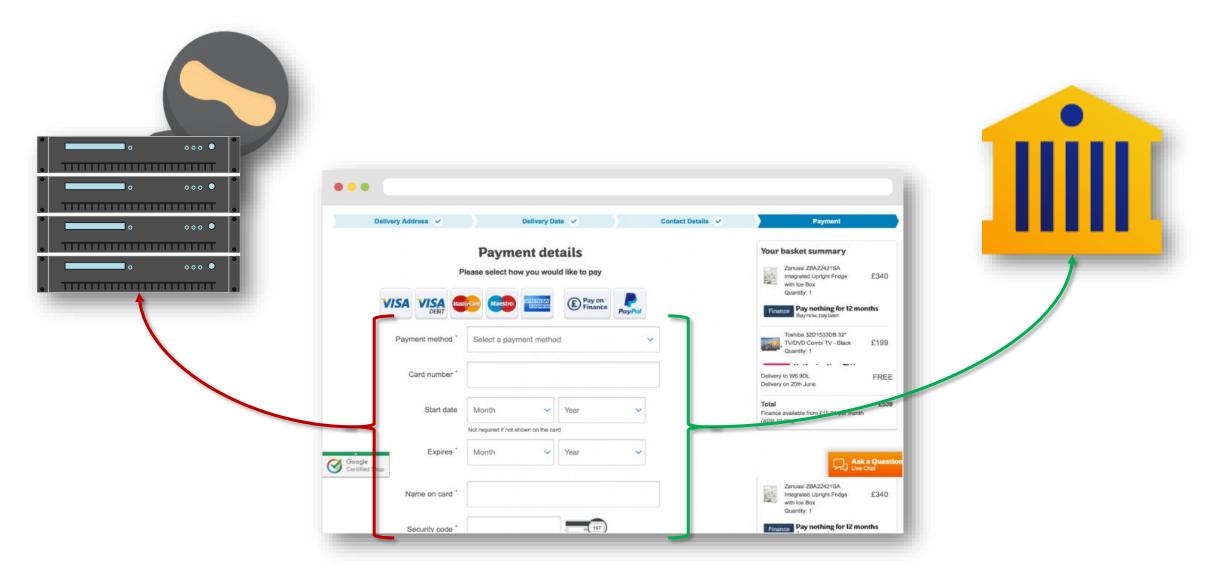




#### How eCommerce Malware Works



### How eCommerce Malware Works





# What Visa is Doing to Help



# Payment Fraud Disruption: At-a-Glance



 Disruption of fraud and crime through early detection and alerting

- Operational prevention and response to client, merchant and third-party breaches
- Advance key law enforcement and industry partnerships, both domestically and internationally

## What Visa Is Doing To Help?



#### 1. eCommerce Threat Disruption (eTD) Initiative

- Proactive compromise detection that doesn't rely on fraud reports
- Shortens the time-to-remediate from months to days
- Works to disrupt attackers by taking down their infrastructure

#### 2. Developing Detection Algorithms

- Advanced machine learning algorithms to identify common points of purchase (CPPs)
- Ability to identify CPPs quicker and at a greater scale

#### 3. Industry Outreach

Webinars, Intelligence Alerts, and Best Practice Guides



# Resources for Merchants and Best Practices

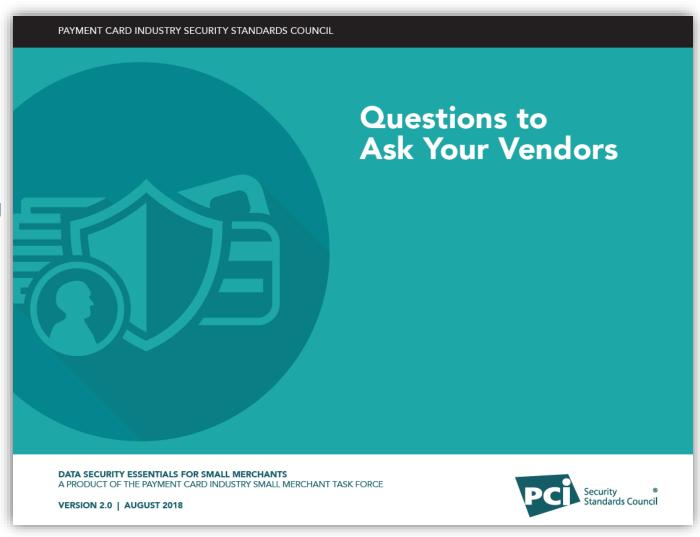


## Payment Card Industry Resources for Small Merchants

www.pcisecuritystandards.org/merchants/#rfsm

- Aids small-merchant owners and operators
- Provides questions to ask your vendors and service providers
- Assists with understanding how vendors support the protection of your customers' card data and your environment
- Is the vendor's solution required? Ensure a strong business justification
- Ask vendor what happens if there is a data breach?
  - ✓ How is the merchant notified?
  - ✓ What monitoring services do they provide?
- Partner with your merchant acquiring bank for guidance

**NOTE:** If a merchant suspects a compromise, they should contact their acquiring bank immediately for guidance to ensure compliance with all Visa investigation and compliance guidelines





## How can merchants protect themselves?

Visa Online Merchant Tool Kit provides helpful information to make a seamless EMV transition

• Streamline your chip migration <a href="www.VisaChip.com/businesstoolkit">www.VisaChip.com/businesstoolkit</a>

Visa Data Security Website <a href="https://www.visa.com/cisp">www.visa.com/cisp</a>

- Alerts, Bulletins
- Best Practices, White Papers
- Past Webinars

Visa Global Registry of Service Providers <a href="https://www.visa.com/onthelist">www.visa.com/onthelist</a>

• List of registered, PCI DSS validated third party agents

PCI Resources for Small Merchants <a href="https://www.pcisecuritystandards.org/merchants/">https://www.pcisecuritystandards.org/merchants/</a>

- Guide to Safe Payments, Common Payment Systems, Questions to Ask your Vendors
- Payment Data Security Essential: Video and Infographics

PCI Security Standards Council Website <a href="www.pcissc.org">www.pcissc.org</a>

Data Security Standards, Qualified Assessor Listings, Data Security Education Materials





#### **Additional Questions?**

Contact <a href="mailto:cisp@visa.com">cisp@visa.com</a>





#### Additional Visa Resources

# Visa has a number of documents for clients to reference Visa Security Alerts (public) www.visa.com/cisp

- "Fraudsters Targeting Call Center Chat and Non-Voice Channels"
  July 2018
- "Protect Against eCommerce Malware" January 2018

#### www.visaonline (non-public)

Payment Fraud Disruption's *Pr3ssure Gauge*,
 April 2018: "Artificial Intelligence: The future of call centers"

#### For more information on Visa Online:

- Payment System Intelligence
- Data Compromise and Fraud Investigations



#### Visa Combats eCommerce Fraud

eCommerce malware compromises are a persistent contributor to global fraud in the Card-Not-Present space.

Visa's eCommerce Threat Disruption program helps identify and disrupt eCommerce merchant compromises before fraud occurs.

#### Core Objective



The main objective of the eCommerce Threat Disruption (eTD) program is to narrow the gap between detection and prevention.

By moving away from detection by fraud reporting toward proactively searching for threats, Visa's Payment Fraud Disruption team is able to notify merchants of compromises before the stolen data is monetized.



Payment Systems Intelligence - Security Bulletin

JANUARY 2018

#### PROTECT AGAINST ECOMMERCE MALWARE

Distribution: Visa Issuers, Acquirers, Processors, and Merchants

#### VISA SECURITY ALERT

**JULY 2018** 

FRAUDSTERS TARGETING CALL CENTER CHAT AND NON-VOICE CHANNELS

#### **DISTRIBUTION: ISSUERS, ACQUIRERS, MERCHANTS AND AGENTS**

#### EXECUTIVE SUMMARY:

A growing industry trend to deploy artificial intelligence (Al) that supports online chat and nonvoice channel services within call centers and merchant online environments may introduce potential risks to the users of these services. According to a recent report by <a href="PYMNTS.com">PYMNTS.com</a>, 85% of all call center interactions will not require a human employee by 2020. Visa Payment Systems Intelligence (PSI) identified increasing instances of criminals targeting these online services to obtain payment data.

Use of chat and non-voice channels can be an efficient method for managing customer interactions, however, the risk of potential exploitation grows if additional anti-fraud and security measures are not used in conjunction with these services. Without proper vetting, these services and software solutions provided by third-parties potentially introduce the risk of logical errors or vulnerabilities that may be discovered and exploited by criminals. The purpose of this Visa Security Alert is to provide clients with an understanding of the threat landscape and best practices for securing this environment.

#### **Targeting Chat and Non-Voice Channels**

Al technology is increasingly important as call centers become the primary customer interaction point for many payment system participants and their clients. Due to the rise in online and mobile commerce, payment system participants and their agents are deploying Al solutions to assist with increasing call volumes. Further, many call centers are also expanding services to help close potential sales. New chatbool and non-voice Al services are used to quickly answer customer questions regarding goods/services and drive users to complete the sale.

o global fraud in the Card-Not-Present space. and persistent attacks, Visa is providing guidance tores

the eCommerce website itself. It does not intend to

ner—similar to physical skimming, card data and can be an appealing and lucrative endeavor for iffords criminals a degree of physical separation from lack of any physical presence. In general, these and persistent. Because of these factors, merchants

een placed into a merchant's website code directly

s domain and is loaded by the merchant's website

mmerce site's server to place their skimming code.

ecurity Alerts from Visa

ng fraud to find the source of dentifying and analyzing the

ire, where Visa identifies

roach allows the eTD

Disruption

rchant/library.html

VISA



## Summary

- Focus: Ecommerce fraud is a growing area of concern
- Capability: eTD allows us to get ahead of fraud, identifying compromises before fraud occurs
- **Value-add:** Tools like eTD provide immediate security benefit for eCommerce merchants globally
- Speed: A cost efficient service for issuers, acquirers and small merchants
  - Faster containment and distribution of at-risk accounts
  - Decreased number of days from identification to case closure





