Payment Fraud Disruption

Webinar: Threats from Website Add-ons and E-commerce Trends

Stoddard Lambertson & Sam Cleveland

Payment Fraud Disruption

September 5, 2018

VISA

Agenda

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

Threat Landscape

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

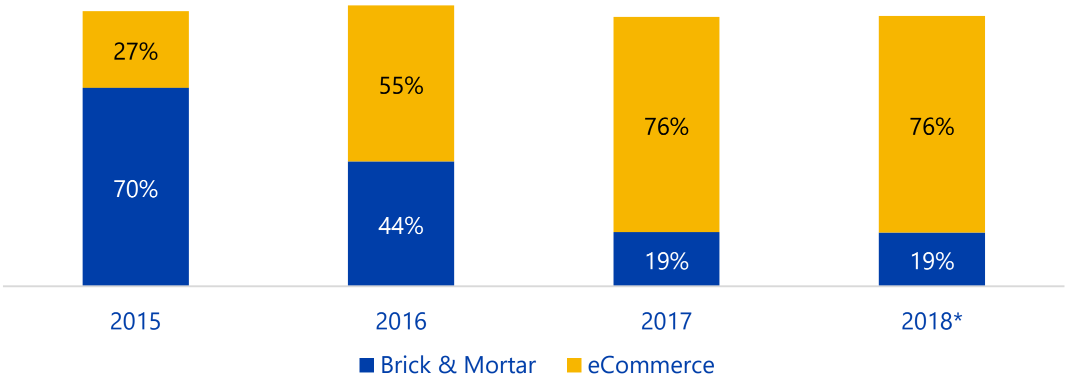
Criminals Moving Beyond Merchants

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

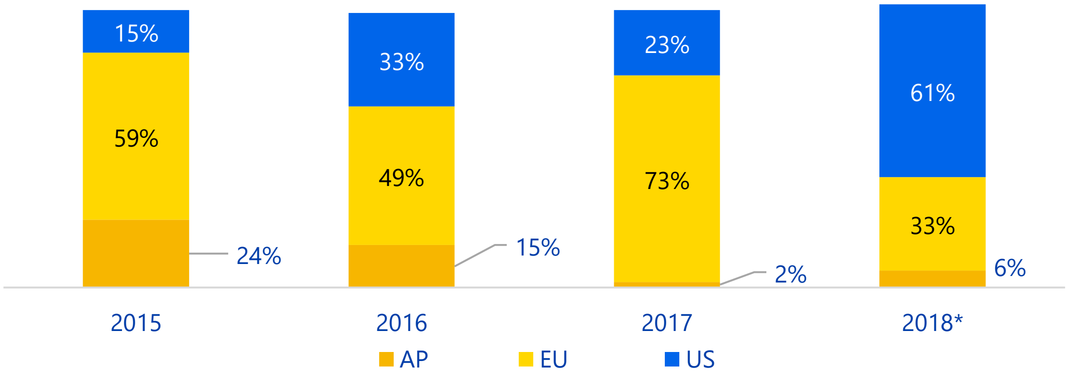
Sharpening Focus on Evolving Trends

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

Unique Cases by Entity Type



Unique eCommerce Cases by Region



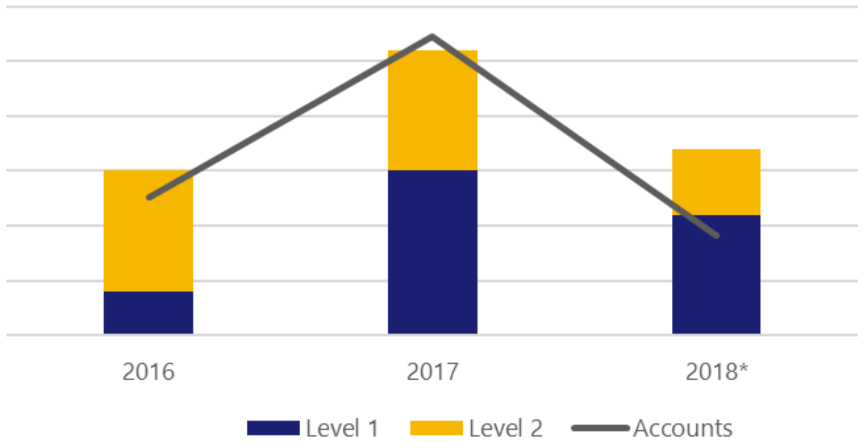
*January 2018 – June 2018

Global Breaches Summary: Q2 2018

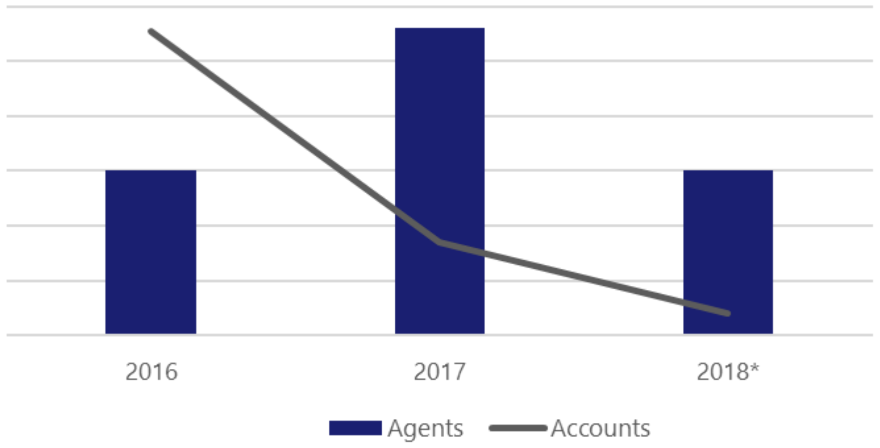
Global Breaches by Level

	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



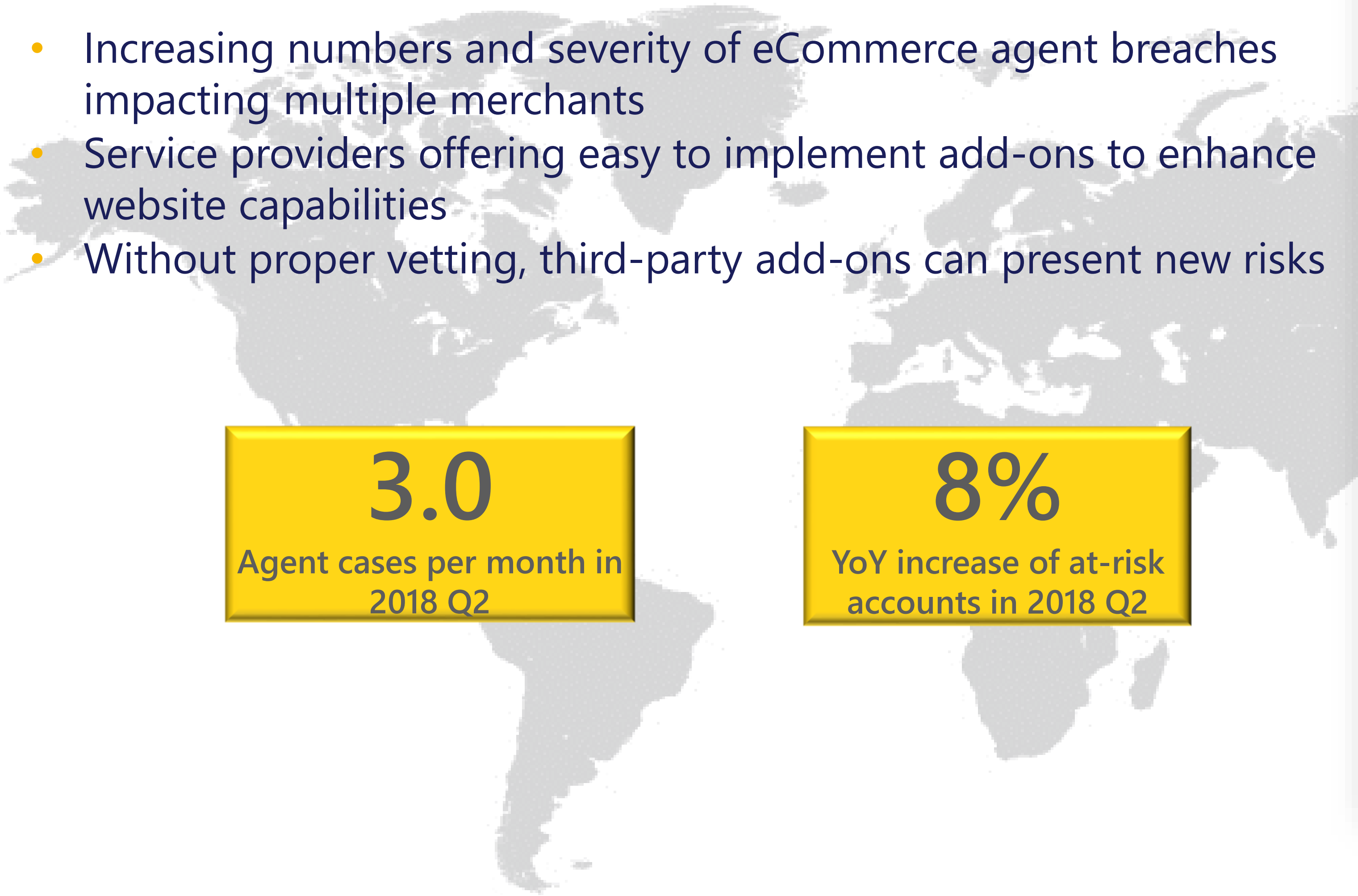
Service Provider Breaches



** Available for 1 January 2018 – 30 June 2018.*
*** Service Provider category includes all agents.*
**** As of 1 January 2018, cases in Europe will be combined with ROW categories.*

The Threat Landscape

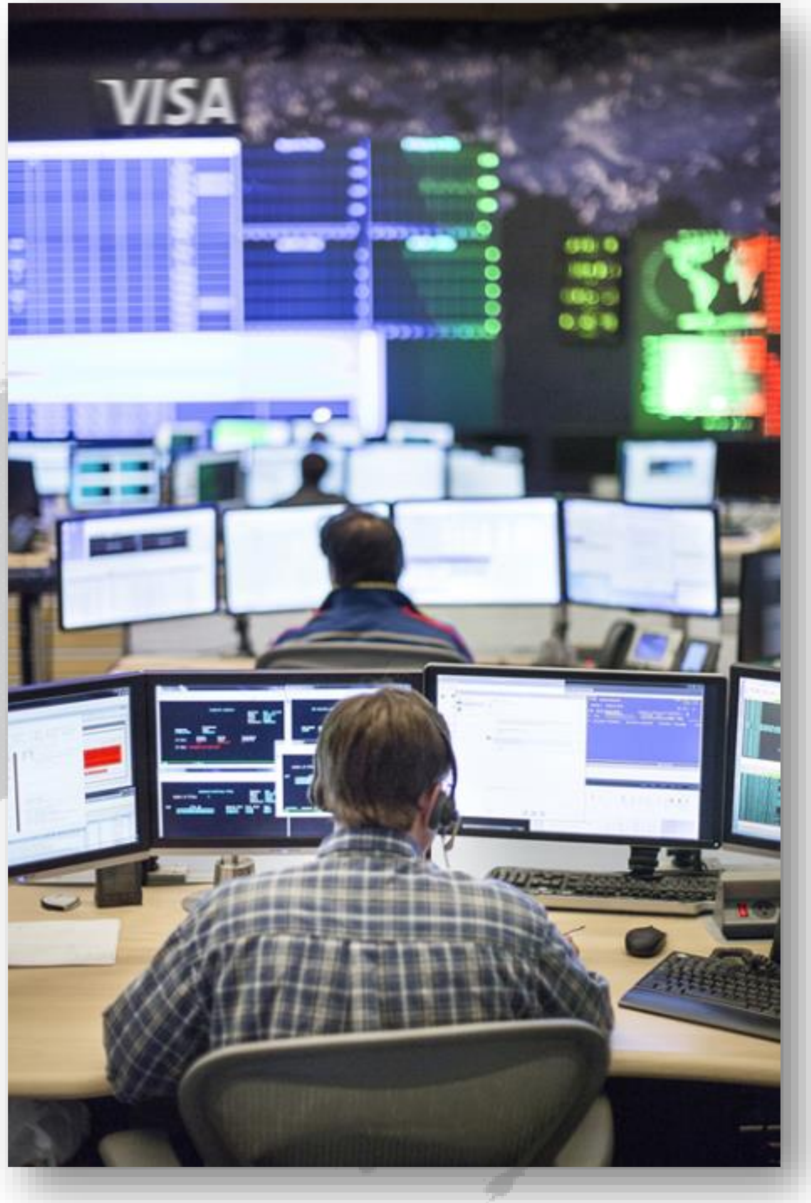
Criminals are migrating to the eCommerce space



- Increasing numbers and severity of eCommerce agent breaches impacting multiple merchants
- Service providers offering easy to implement add-ons to enhance website capabilities
- Without proper vetting, third-party add-ons can present new risks

3.0
Agent cases per month in 2018 Q2

8%
YoY increase of at-risk accounts in 2018 Q2



Criminals Targeting the eCommerce Channel

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.

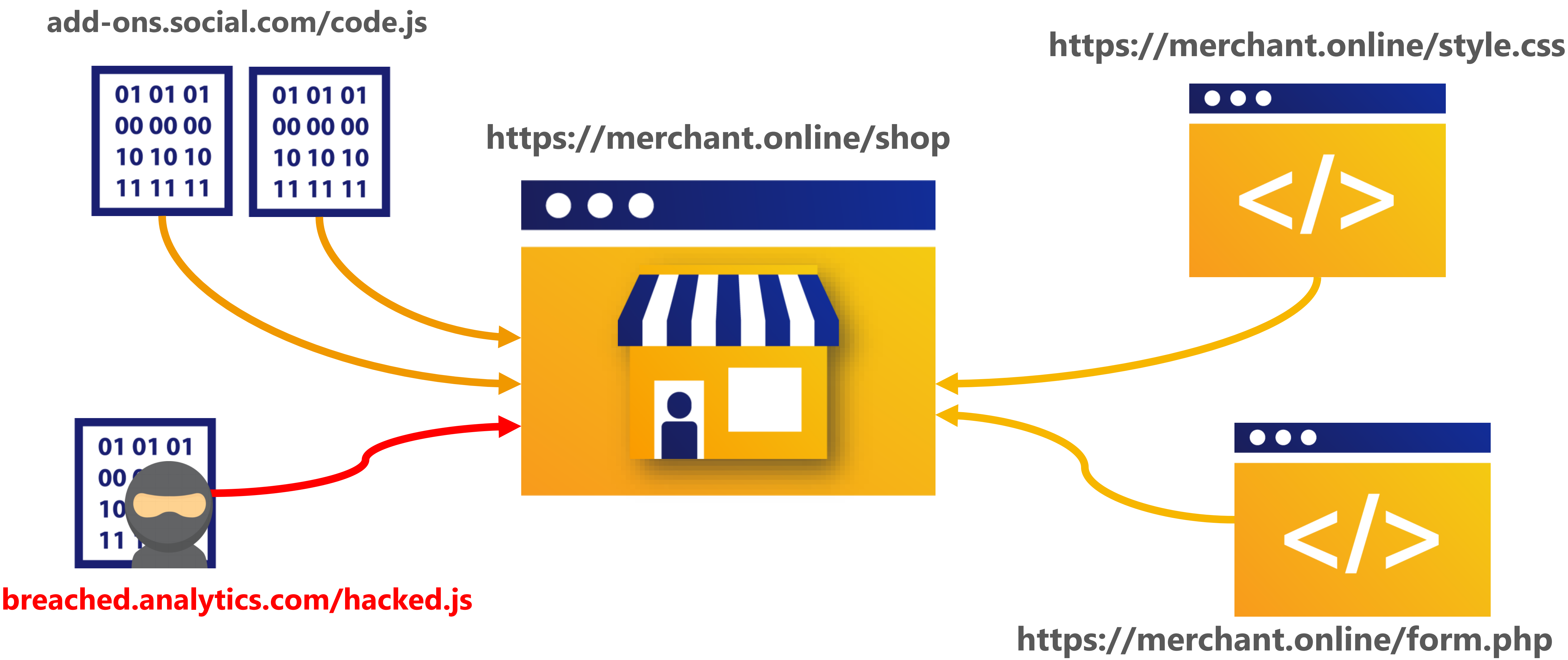
What risks do website plugins and scripts pose?

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 plug-in 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

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

How eCommerce Malware Works



add-ons.social.com/code.js

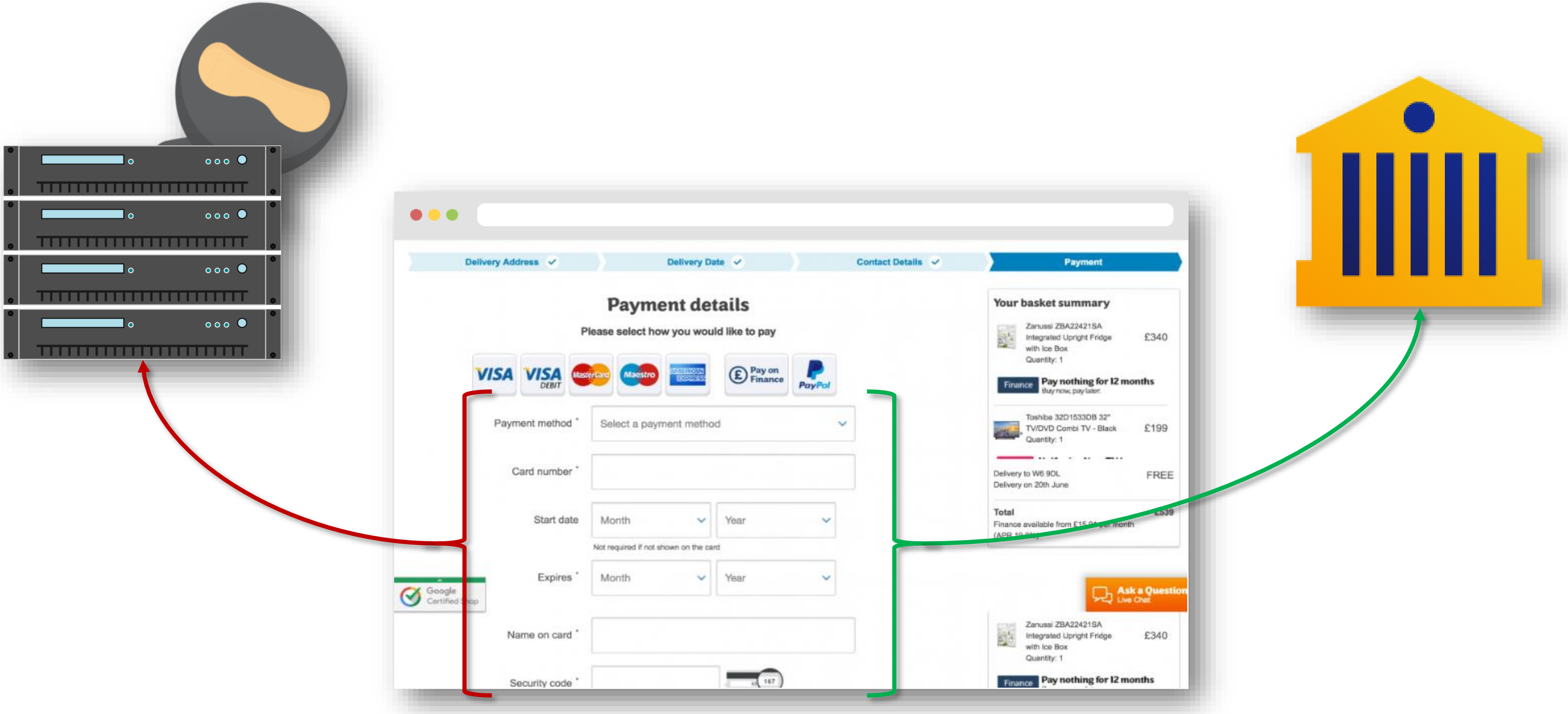
https://merchant.online/style.css

https://merchant.online/shop

breached.analytics.com/hacked.js

https://merchant.online/form.php

How eCommerce Malware Works



Delivery Address ✓ | Delivery Date ✓ | Contact Details ✓ | Payment

Payment details

Please select how you would like to pay

Payment method * Select a payment method

Card number *

Start date Month Year

Not required if not shown on the card

Expires * Month Year

Name on card *

Security code *

Your basket summary

Zanussi ZBA22421SA Integrated Upright Fridge with Ice Box Quantity: 1	£340
Finance **Pay nothing for 12 months** Buy now, pay later.	
Toshiba 32D1533DB 32" TV/DVD Combi TV - Black Quantity: 1	£199
Delivery to W6 9DL Delivery on 20th June	FREE
Total Finance available from £15.[illegible] per month (APR [illegible])	£539

Zanussi ZBA22421SA Integrated Upright Fridge with Ice Box Quantity: 1	£340
Finance **Pay nothing for 12 months**	

What Visa is Doing to Help

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

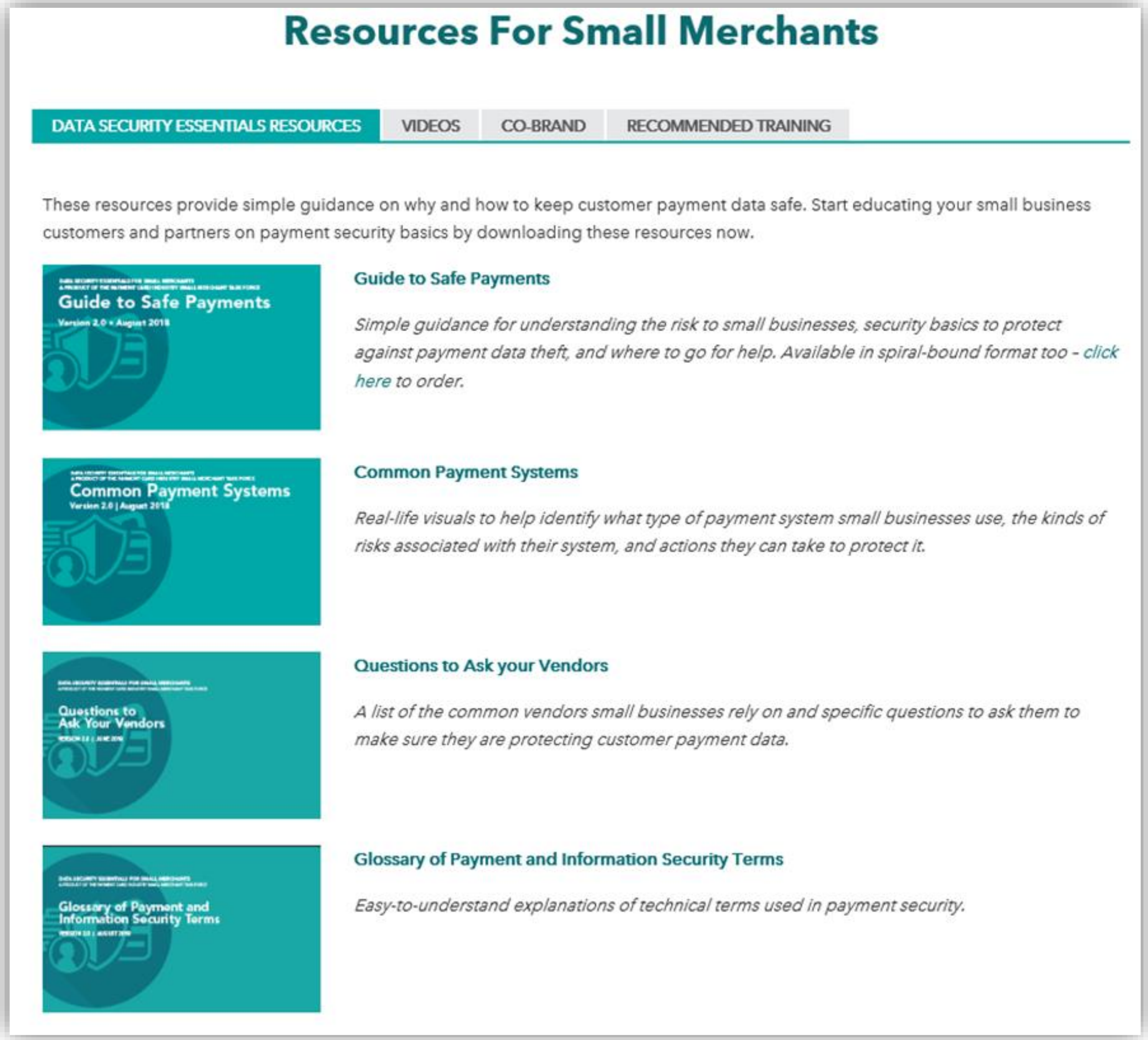
Resources for Merchants and Best Practices

Payment Card Industry Resources for Small Merchants

www.pcisecuritystandards.org/merchants/#rfsm

Educational Resources Include:

- ✓ Guide To Safe Payments
- ✓ Common Payment Systems
- ✓ Questions To Ask Your Vendors?
- ✓ Glossary of Security Terms



Resources For Small Merchants

These resources provide simple guidance on why and how to keep customer payment data safe. Start educating your small business customers and partners on payment security basics by downloading these resources now.

Guide to Safe Payments
Version 2.0 • August 2018

Guide to Safe Payments

Simple guidance for understanding the risk to small businesses, security basics to protect against payment data theft, and where to go for help. Available in spiral-bound format too - click here to order.

Common Payment Systems
Version 2.0 | August 2018

Common Payment Systems

Real-life visuals to help identify what type of payment system small businesses use, the kinds of risks associated with their system, and actions they can take to protect it.

Questions to Ask Your Vendors

Questions to Ask your Vendors

A list of the common vendors small businesses rely on and specific questions to ask them to make sure they are protecting customer payment data.

Glossary of Payment and Information Security Terms

Glossary of Payment and Information Security Terms

Easy-to-understand explanations of technical terms used in payment security.

Payment Card Industry Guide to Safe Payments

www.pcisecuritystandards.org/pdfs/Small_Merchant_Guide_to_Safe_Payments.pdf

- Understanding Merchant Risks
- Helps e-Commerce merchants understand their payment systems
- Describes how to protect your business with risk reduction security basic recommendations
- Recommends use of ***trusted business partners*** and know how to contact them
  - Understanding your business partners beyond payments

Payment Card Industry Security Standards Council

DATA SECURITY ESSENTIALS FOR SMALL MERCHANTS
A PRODUCT OF THE PAYMENT CARD INDUSTRY SMALL MERCHANT TASK FORCE

Guide to Safe Payments

Version 2.0 • August 2018

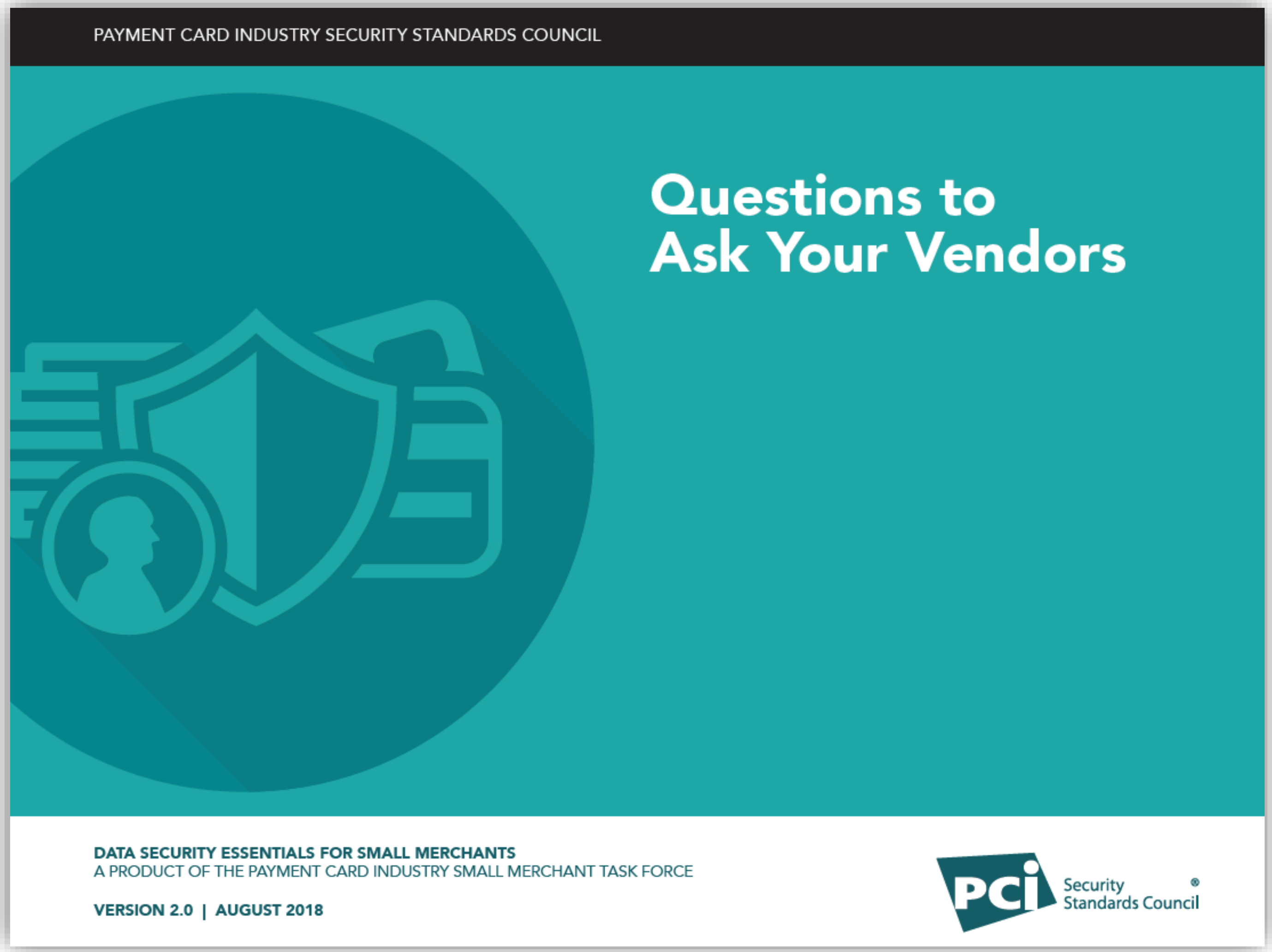
PCI Security Standards Council®

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*



PAYMENT CARD INDUSTRY SECURITY STANDARDS COUNCIL

Questions to Ask Your Vendors

DATA SECURITY ESSENTIALS FOR SMALL MERCHANTS
A PRODUCT OF THE PAYMENT CARD INDUSTRY SMALL MERCHANT TASK FORCE

VERSION 2.0 | AUGUST 2018

PCI Security Standards Council®

How can merchants protect themselves?

Additional Questions?
Contact cisp@visa.com

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

- Streamline your chip migration www.VisaChip.com/businesstoolkit

Visa Data Security Website www.visa.com/cisp

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

Visa Global Registry of Service Providers www.visa.com/onthelist

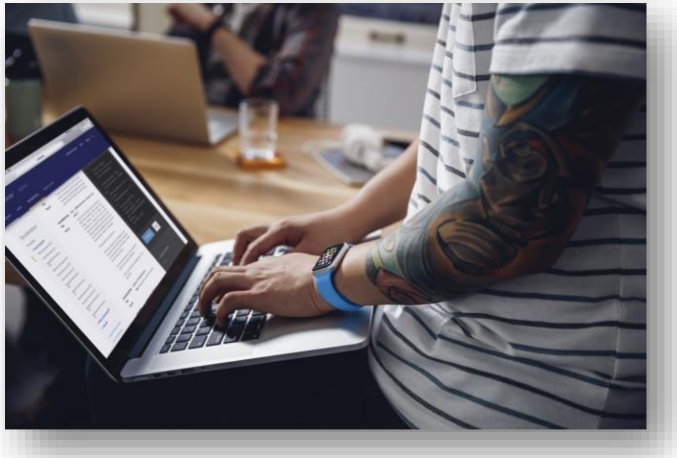
- List of registered, PCI DSS validated third party agents

PCI Resources for Small Merchants https://www.pcisecuritystandards.org/merchants/

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

PCI Security Standards Council Website www.pcissc.org

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



pci DSS CERTIFIED

Visa Global Registry of Service Providers | www.visa.com/onthelist
For details, see
On the list! 2017
Supports Secure Technology

Additional Visa Resources

Visa has a number of documents for clients to reference

Visa Security Alerts (public) www.visa.com/cisp

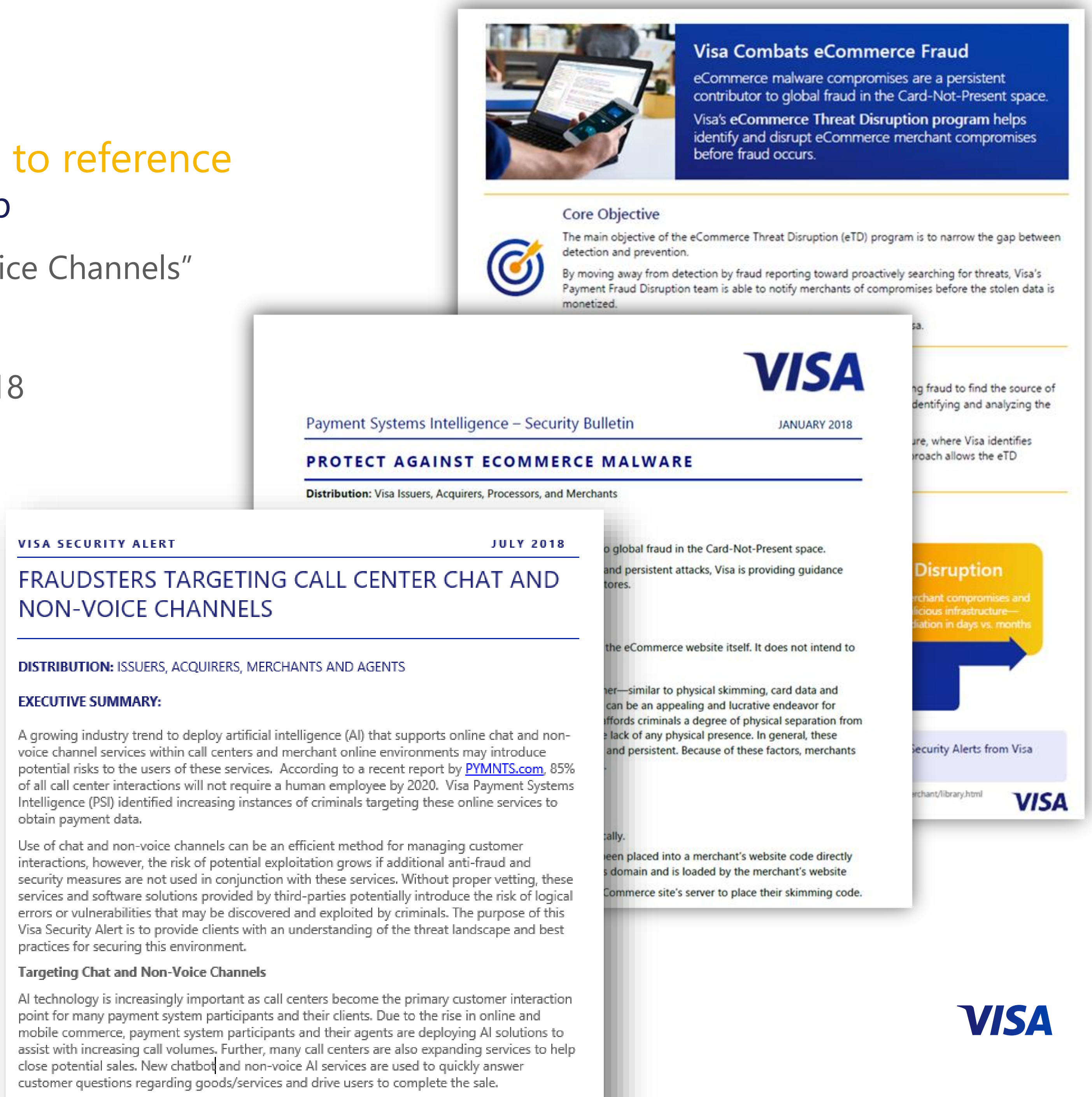
- “Fraudsters Targeting Call Center Chat and Non-Voice Channels” July 2018
- “Protect Against eCommerce Malware” January 2018

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.

sa.

ng fraud to find the source of dentifying and analyzing the

ure, where Visa identifies roach allows the eTD

Disruption

rchant compromises and licious infrastructure— diation in days vs. months

Security Alerts from Visa

rchant/library.html

VISA

VISA

Payment Systems Intelligence – Security Bulletin JANUARY 2018

PROTECT AGAINST ECOMMERCE MALWARE

Distribution: Visa Issuers, Acquirers, Processors, and Merchants

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 affords criminals a degree of physical separation from lack of any physical presence. In general, these and persistent. Because of these factors, merchants

cally.

een placed into a merchant’s website code directly s domain and is loaded by the merchant’s website

Commerce site’s server to place their skimming code.

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 (AI) that supports online chat and non-voice 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 PYMNTS.com, 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

AI 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 AI solutions to assist with increasing call volumes. Further, many call centers are also expanding services to help close potential sales. New chatbot and non-voice AI services are used to quickly answer customer questions regarding goods/services and drive users to complete the sale.

VISA

Q&A