Payment Fraud Disruption

Webinar: Threats from Website Add-ons and E-commerce Trends
Stoddard Lambertson & Sam Cleveland

Payment Fraud Disruption
September 5, 2018
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**

<table>
<thead>
<tr>
<th>Year</th>
<th>Brick &amp; Mortar</th>
<th>eCommerce</th>
</tr>
</thead>
<tbody>
<tr>
<td>2015</td>
<td>70%</td>
<td>27%</td>
</tr>
<tr>
<td>2016</td>
<td>44%</td>
<td>55%</td>
</tr>
<tr>
<td>2017</td>
<td>19%</td>
<td>76%</td>
</tr>
<tr>
<td>2018*</td>
<td>19%</td>
<td>76%</td>
</tr>
</tbody>
</table>

**Unique eCommerce Cases by Region**

<table>
<thead>
<tr>
<th>Year</th>
<th>AP</th>
<th>EU</th>
<th>US</th>
</tr>
</thead>
<tbody>
<tr>
<td>2015</td>
<td>24%</td>
<td>15%</td>
<td>59%</td>
</tr>
<tr>
<td>2016</td>
<td>15%</td>
<td>49%</td>
<td>33%</td>
</tr>
<tr>
<td>2017</td>
<td>15%</td>
<td>73%</td>
<td>2%</td>
</tr>
<tr>
<td>2018*</td>
<td>33%</td>
<td>33%</td>
<td>61%</td>
</tr>
</tbody>
</table>

*January 2018 – June 2018
Global Breaches Summary: Q2 2018

Global Breaches by Level

<table>
<thead>
<tr>
<th></th>
<th>2015</th>
<th>2016</th>
<th>2017</th>
<th>2018*</th>
</tr>
</thead>
<tbody>
<tr>
<td>Level 1</td>
<td>&lt;1%</td>
<td>&lt;1%</td>
<td>2%</td>
<td>4%</td>
</tr>
<tr>
<td>Level 2</td>
<td>&lt;1%</td>
<td>1%</td>
<td>1%</td>
<td>2%</td>
</tr>
<tr>
<td>Level 3</td>
<td>4%</td>
<td>13%</td>
<td>15%</td>
<td>28%</td>
</tr>
<tr>
<td>Level 4</td>
<td>76%</td>
<td>57%</td>
<td>38%</td>
<td>60%</td>
</tr>
<tr>
<td>Service Provider**</td>
<td>2%</td>
<td>2%</td>
<td>4%</td>
<td>6%</td>
</tr>
<tr>
<td>Europe***</td>
<td>17%</td>
<td>27%</td>
<td>39%</td>
<td>-</td>
</tr>
<tr>
<td>Total</td>
<td>100%</td>
<td>100%</td>
<td>100%</td>
<td>100%</td>
</tr>
</tbody>
</table>

Large Merchant Breaches

Service Provider Breaches

** 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 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 as a merchant’s own eCommerce environment.

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.
How eCommerce Malware Works

Add-ons.social.com/code.js

https://merchant.online/shop

Breached.analytics.com/hacked.js

https://merchant.online/style.css

https://merchant.online/form.php
How eCommerce Malware Works
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
Payment Card Industry Guide to Safe Payments


- 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 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

Visa Data Security Website [www.visa.com/cisp](http://www.visa.com/cisp)
- Alerts, Bulletins
- Best Practices, White Papers
- Past Webinars

Visa Global Registry of Service Providers [www.visa.com/onthelist](http://www.visa.com/onthelist)
- List of registered, PCI DSS validated third party agents

PCI Resources for Small Merchants [https://www.pcisecuritystandards.org/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](http://www.pcissc.org)
- Data Security Standards, Qualified Assessor Listings, Data Security Education Materials

Additional Questions?
Contact [cisp@visa.com](mailto:cisp@visa.com)
Additional Visa Resources

Visa has a number of documents for clients to reference:

**Visa Security Alerts (public)** [www.visa.com/cisp](http://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