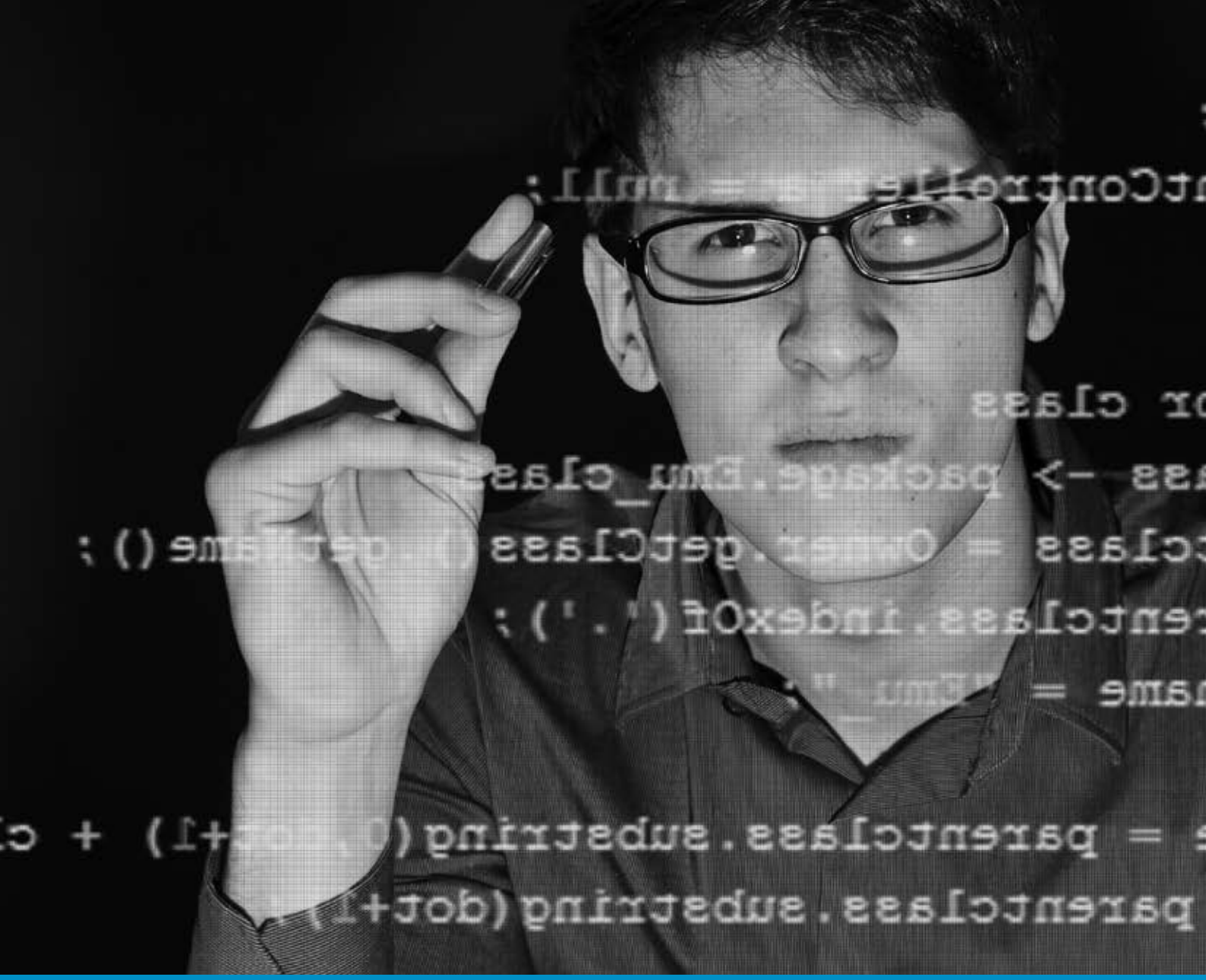
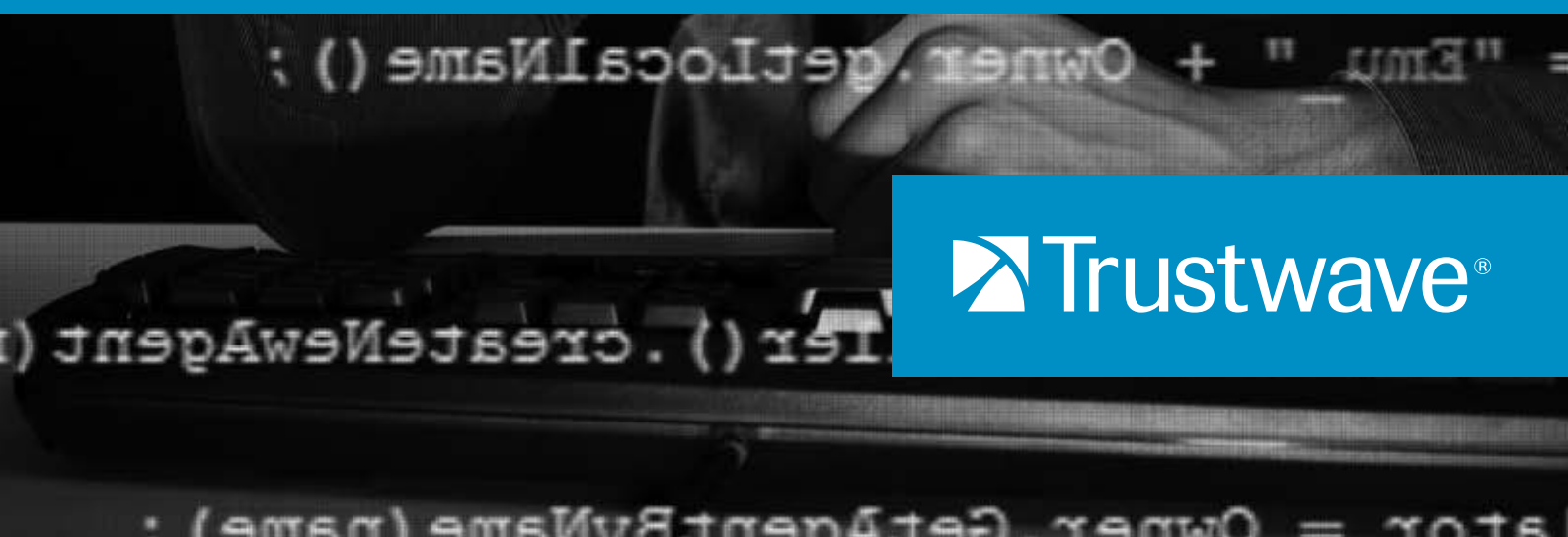


PCI Forensics Investigation

A HANDBOOK FOR SMALL MERCHANTS



Trustwave®

Table of Contents

Trustwave SpiderLabs

EXPERTISE AND EXPERIENCE

Trustwave SpiderLabs is the advanced security team within Trustwave focused on application security, incident response, penetration testing, physical security and security research—including anti-malware and threat intelligence. Trustwave SpiderLabs has performed more than 1,500 incident response investigations, thousands of penetration tests, and hundreds of application security tests.

With more than eight years of service, Trustwave SpiderLabs is uniquely positioned to help many organizations respond to and resolve a variety of security incidents. Our team members are experienced security professionals, with career experience ranging from corporate information security and security research, to federal and local law enforcement.

Trustwave SpiderLabs is a member of FIRST, the global Forum for Incident Response and Security Teams. FIRST is the premier organization and recognized global leader in incident response. Membership in FIRST enables incident response teams to more effectively respond reactively and proactively to security incidents.

As an active member of the incident response community, Trustwave SpiderLabs is a member of the International Association of Financial Crime Investigators (IAFCI), International Association of Chiefs of Police (IACP) and participates in the U.S. Secret Service's Electronic Crimes Task Forces (ECTF).

Trustwave®
SpiderLabs®

Compromised! Now what?

Learning that an intruder has accessed your system and stolen sensitive data can be a shock. You might feel violated and maybe even anxious about the investigation. Rest assured that you are not the first, only or last organization to experience a data compromise—you are not alone. Trustwave has investigated more than 1,500 data compromises and helped organizations large and small navigate the process. Trustwave is here to help.

This handbook is a PCI Forensics Investigation intended to help small merchants navigate through the steps to take to complete the PCI forensics investigation process after a data compromise takes place.

How did the bank know about the compromise?

If your bank contacted you, your business was probably identified as a Common Point-of-Purchase (CPP). When the payment brands (i.e., Visa Inc., MasterCard Worldwide, American Express, Discover Network and JCB) analyze reports of fraudulent card activity and find that a number of compromised cards were used at the same place of business during a certain period of time, those businesses are included in a CPP report. As a result of that report, your processing bank contacted you.

Regardless of the cause of the breach, you must now hire an approved PCI Forensic Investigator (PFI) company to investigate the breach and inform you of any actions you must take to secure your payment card environment.

Why should I cooperate with the investigation?

You will find that cooperating with the investigation without delay will be in your best interest:

- Any delay in containing the damage and limiting exposure could further damage your reputation and, in some cases, increase the amount of related fines and fees you may need to pay (see “How to Contain Damage and Limit Exposure” on the next page of this document).
- You will likely be fined or penalized by the card brands via your acquiring bank and impeding the containment of the compromise could result in increased fines.
- Your payment system is now a crime scene. As your computer system continues to operate, it could destroy or taint evidence that could help define when, where and how your system was breached.

How will I work with Trustwave?

Your work with Trustwave SpiderLabs will begin with either you or your acquiring bank engaging Trustwave for PFI services. Trustwave will then assign a SpiderLabs investigator to your case. That individual will lead the investigation, act as your adviser throughout the process and support you in your communications with your bank, the card brands or your acquirer. Usually on the same day the case is assigned, the investigator will contact you to find out more about the case, answer your questions and schedule an on-site visit.

Please note that the due to perceived conflict of interest, the vendor performing your PCI compliance should not be also doing your PFI. So if Trustwave is performing your PCI then we cannot also do your PFI. However, in the event that you have us do your PFI then after the investigation is complete, we can assist with your PCI compliance.

Business relationships and responsibilities

It's important to understand that, depending on the card brand, responsibility and liability can vary.

In terms of MasterCard and Visa, you have a contract in place with your processing bank that allows you to accept MasterCard and Visa payments. You don't have a direct relationship with MasterCard or Visa. Your bank does, and this makes the bank responsible for making sure that you are compliant with the Payment Card Industry Data Security Standard (PCI DSS), therefore you will report PCI DSS compliance status to your bank.

If you also accept American Express or Discover payments, you probably have a direct relationship with them because they act as both the processor and the card brand. In this type of situation, you will report your PCI DSS compliance status directly to the brand.

How to contain damage and limit exposure

You should adhere to the following items to the extent possible:

- Do not access or alter compromised system(s).
- Do not log on to compromised systems or change passwords.
- Do not turn the system off, and if possible, isolate it from the network.
- If accessing the compromised system(s) can't be avoided for business reasons, ensure that you keep detailed records describing any actions you take and the date and time you take them.
- Preserve logs – make sure systems are configured to retain logs and not delete or overwrite them..
- Be on high alert and monitor traffic on all systems that handle cardholder data.
- If you have a wireless network, change the Service Set Identifier (SSID) on the Wireless Access Point (WAP) and systems that use the WAP, but do not change this information on any compromised systems.

What will happen during the on-site investigation?

Depending on the specifics of the compromise, the card brands may require an on-site investigation. If an on-site investigation is required, Trustwave must be on-site within five business days of our receiving the case assignment, regardless of your location.

When the investigator arrives on-site, he or she will meet with you to gather more details and address any concerns or questions you may have. Because a compromise is a sensitive topic, the investigator will try not to draw any attention to his or herself. Organizations usually do not like to bring attention to the fact that the business has been compromised and usually say the investigators are there to perform an IT security audit.

The investigator will need physical access to the systems suspected to have been compromised and will require administrator user names and passwords. Once you provide access, little more will be required of you during the on-site investigation.

In more complex network environments, the investigator may need an IT staff member on-site to help ensure proper identification of the systems and access to them.

What exactly will the investigator be doing?

The investigator will review your environment, perform a live analysis and create forensic images of suspect system hard drives. Whenever possible, the investigator will make a live copy of your systems to avoid any network downtime—Trustwave investigators understand the need for business to continue to operate as normal. If downtime cannot be avoided, it will be scheduled for a time that will have the least impact on your business, regardless of the time of day.

If it's required, how long will the investigator be on-site?

Many factors affect how long an investigator needs to be on-site, such as the age of the systems, size of affected hard drives and number of affected systems. For a small retail environment, Trustwave may be on-site for the length of a typical workday. During this time we will make every effort to keep your business running normally.

What is a live analysis?

While on-site, the investigator will perform a live analysis that includes, but is not limited to, analyses of your system memory, any malware on the system, the timeline of the compromise, files and logs. These analyses allow the investigator to develop a sound theory about what happened before he or she leaves the site. The investigator will share his or her findings with the appropriate on-site contact or manager and provide a copy of the evidence acquired for your records in the event that any legal or law enforcement actions take place.

What can I do next? Initial remediation

Once the investigator has imaged your system's hard drives, you can begin to take initial remediation actions and start to correct outstanding security deficiencies. Usually, you will need to correct a number of deficiencies, and you will want to stay organized.

We recommend that you create a task list or spreadsheet including all deficiencies, a target date for the resolution of each deficiency and the actual completion date. This list will help you be proactive and keep your bank informed with weekly status reports (see page 8 of this document for more information about your task list).

What happens after the on-site investigation?

Once the investigator finishes the on-site work, he or she will return to a Trustwave SpiderLabs facility. There, the evidence will be backed-up and secured in a fire-proof vault with strict access controls. The investigator then works from a copy of the evidence and uses state-of-the-art hardware and software tools at the facility to complete the investigation.

All Trustwave SpiderLabs team members are certified as Qualified Security Assessors (QSAs) and follow strict fraud control and investigations procedures as outlined by Visa in the document "What To Do If Compromised" available at http://usa.visa.com/download/merchants/cisp-what-to-do-if-compromised.pdf.

The investigator must issue a preliminary report no more than five days after arriving at Trustwave SpiderLabs facilities. The preliminary report may be six or more pages long depending on the size and complexity of the breach. The report is only preliminary and things could change as more information comes to light, but the report will include what the investigator currently knows and a summary of possible causes.

Are the perpetrators ever apprehended?

Yes. At your request we will reach out to the appropriate authorities. We regularly work with the U.S. Secret Service, Interpol, and state and federal law enforcement and know how to help support their efforts. When evidence from an investigation includes actionable intelligence, it can support law enforcement in apprehending the individuals responsible for the breach.

What is included in the final report?

The investigation culminates in the issuance of a final report detailing all investigation findings. The final report is issued a few weeks after the preliminary report, depending on the scope of the investigation.

Both the card brands and your bank require a final report that will include:

- System and network deficiencies
- Findings
- Timeframe of exposure
- Windows of intrusion
- Number of cards at risk
- Outstanding security remediation efforts

Who receives reports?

As discussed previously, the investigation will result in two reports: the preliminary report and the final report. As a PFI, Trustwave SpiderLabs must release reports to all involved parties. Usually, we issue reports simultaneously to you, your bank and any affected card brands.

The final call process

If your bank requires your participation in a final call, the call normally lasts between 30 and 45 minutes and unfolds as outlined below:

1. You should dial in to the call five minutes early.
2. Your bank will take roll call.
3. Your bank will then hand the call over to the investigator.
4. The investigator will review highlights of the report.
5. The investigator will ask you about the status of any outstanding remediation items—submitting a status report prior to the final call will decrease the number of questions you must answer.
6. Before the call ends, time will be allowed for questions—if you have any questions, ask the investigator before the final call and wait to ask questions regarding fines or penalties as you will discuss these issues on a separate call with your bank.

Life after the final call

At this point, you will contact your bank for any additional information regarding the case or related inquiries. By now you should have already provided your bank with the status of any outstanding remediation work. While preferences vary, most banks like to see weekly remediation status reports. The bank wants to ensure your compliance with the PCI DSS as quickly as possible. Failure to complete required remediation items could result in additional fines.

About fines

We do not speak in absolutes in regards to fines. Fines may be levied 30 to 90 days after the close of investigation and any details are NOT shared with Trustwave. There are two types of fines: noncompliance and fraud recovery. For more information on fines, please contact your bank.

What sort of remediation is expected of me?

Complying with PCI DSS requirements is a continuous process that requires on-going maintenance. If the investigation confirms a compromise of your system, your merchant level may escalate and you may be required to fulfill more stringent PCI DSS validation requirements for at least 12 months. To assist you with managing your validation project, Trustwave will provide you a 12-month subscription to our TrustKeeper PCI Manager service. TrustKeeper will be provided towards the end of the investigation once you have been proivided with the recommended remediation actions.

Tracking remediation status

Prior to the final call, you should create a remediation status report document that includes a remediation plan and timeline.

Your remediation status document should include the deficiency, completion status and projected completion date. You'll save yourself time and frustration by being proactive and creating the remediation tracking document as soon as possible. Depending on their complexity, you may be able to correct some items right away, but some items will require more planning and take some time.

As part of our investigation services, Trustwave provides you with 12 months of TrustKeeper® PCI Manager access. TrustKeeper PCI Manager is an on-demand, Web-based compliance and vulnerability management tool that includes reporting options to support compliance and track remediation activity.

Continuous PCI DSS compliance

The PCI DSS requirements can be a little overwhelming, and chances are you might not fully understand some of the requirements. Don't worry, you're not alone.

Your first step in becoming compliant should be identifying the person who's going to take ownership of this process. This person should be someone with some technical skills who understands or can interpret the PCI DSS guidelines.

If you use an outside IT service provider, do not assume that he or she has PCI DSS knowledge or has built your payment environment around PCI DSS guidelines.

In a majority of our cases, it's all too common to hear: "But I pay them to handle my network and security." Please be aware that outsourced IT service providers also need to be PCI DSS compliant—it's required! They should be able to supply you with documentation to support this.

Complying with the PCI DSS may be the best defense you have against another compromise. In order to comply, you will need to validate your compliance on an annual basis and undergo network vulnerability scans each quarter.

If you have an Internet connection and process payments in any way other than using a dial terminal, you may also want to use a tool such as Trustwave's TrustKeeper Agent. This tool helps you monitor compliance on an on-going basis, acting as a "beaconing" device that sends information about the system on which it is installed to TrustKeeper. TrustKeeper Agent can also detect prohibited data and make it easier to scan remote locations that use dynamic IP addresses.

If you need assistance in becoming PCI DSS compliant, Trustwave does offer a variety of services that will aid in the process to help ensure full and continuous compliance.

What reports and documents will my bank need to see?

Usually, a bank will want to see weekly updates to your remediation status document to ensure compliance. We strongly recommend that you provide an update to the bank prior to the final call to

show you are being proactive and make sure your bank is informed when speaking with the card brands. Additionally, an existing remediation plan will help the final call proceed smoothly because both the bank and the card brands will already understand the plan.

Additional documents your bank may request

Once the investigation is complete, your merchant bank will likely request several documents to satisfy PCI DSS compliance requirements:

- Passing TrustKeeper Vulnerability Scan Report
- Completed Self-Assessment Questionnaire (SAQ)
- Completed Attestation of Compliance (AOC)

Trustwave's PCI Manager can help you complete and submit the first two documents. You can get started

with TrustKeeper PCI Manager in one of three ways:

1. You may be part of a program already with your bank or processor. If you already have an account, simply login at https://login.trustwave.com/.
2. If you've not yet activated via your bank's program, visit https://pci.trustwave.com and enter the name of your bank.
3. If you are not affiliated with a bank program and need an account, please visit https://pci.trustwave.com/pci and click "Get Started" to sign up for the service.

Conclusion

By now you should have a good idea of what to expect during the investigation and remediation process. You will receive or be responsible for several items, including:

- ☑ A copy of evidence acquired
- ☑ The preliminary report
- ☑ A remediation status document
- ☑ The final report
- ☑ If required by your bank, the final call
- ☑ Passing TrustKeeper Vulnerability Scan Report
- ☑ Completed Self-Assessment Questionnaire (SAQ)
- ☑ Completed Attestation of Compliance (AOC)

Once you have established access, you will be able to schedule an external vulnerability scan of your environment and complete the Self-Assessment Questionnaire (SAQ). The Passing TrustKeeper Vulnerability Scan Report and SAQ can then be downloaded and supplied to your bank.

Depending on the TrustKeeper solution you choose, you may need to download the Attestation of Compliance (AOC) from a separate website: https://www.pcisecuritystandards.org/saq/index.shtml.

Breach Protection

Many merchants receive breach protection as part of their acquiring bank or ISO's PCI program. You'll need to confirm if you are covered with your acquiring bank. If your program includes breach protection, Trustwave provides either $50,000 or $100,000 of breach protection that covers the following expenses up to that amount:

- The mandatory forensic audit required by the Payment Card Industry Data Security Standard (PCI DSS) when a data breach is suspected (this audit confirms whether an actual breach has occurred and pinpoints where systems are most vulnerable)
- Credit card replacement costs and related expenses
- Assessments and fines levied by card sponsors for data breaches

Please note that the due to perceived conflict of interest, if Trustwave provides breach protection then we cannot also do your PFI. Check with your bank for details of your program. If breach coverage is included in your bank's Trustwave package, please visit http://www.royalgroupservices.com/trustwave/ for instructions on submitting a claim or managing an existing one. You can also print evidence of account protection from this site (you'll need your merchant ID).

Useful links

American Express

www.americanexpress.com/datasecurity

Discover

http://www.discovernetwork.com/fraudsecurity/disc.html

JCB

http://partner.jcbcard.com/security/jcbprogram/

MasterCard

http://www.mastercard.com/us/merchant/pdf/Security_Rules_Merchant_10_17_08.pdf

PCI Security Standards Council

https://www.pcisecuritystandards.org/

Visa

https://usa.visa.com/dam/VCOM/download/merchants/cisp-what-to-do-if-compromised.pdf
http://www.visaeurope.com/en/about_us/security.aspx

Visa USA PCI

https://usa.visa.com/support/small-business/security-compliance.html?ep=v_sym_cisp

https://www.visaeurope.com/receiving-payments/security/