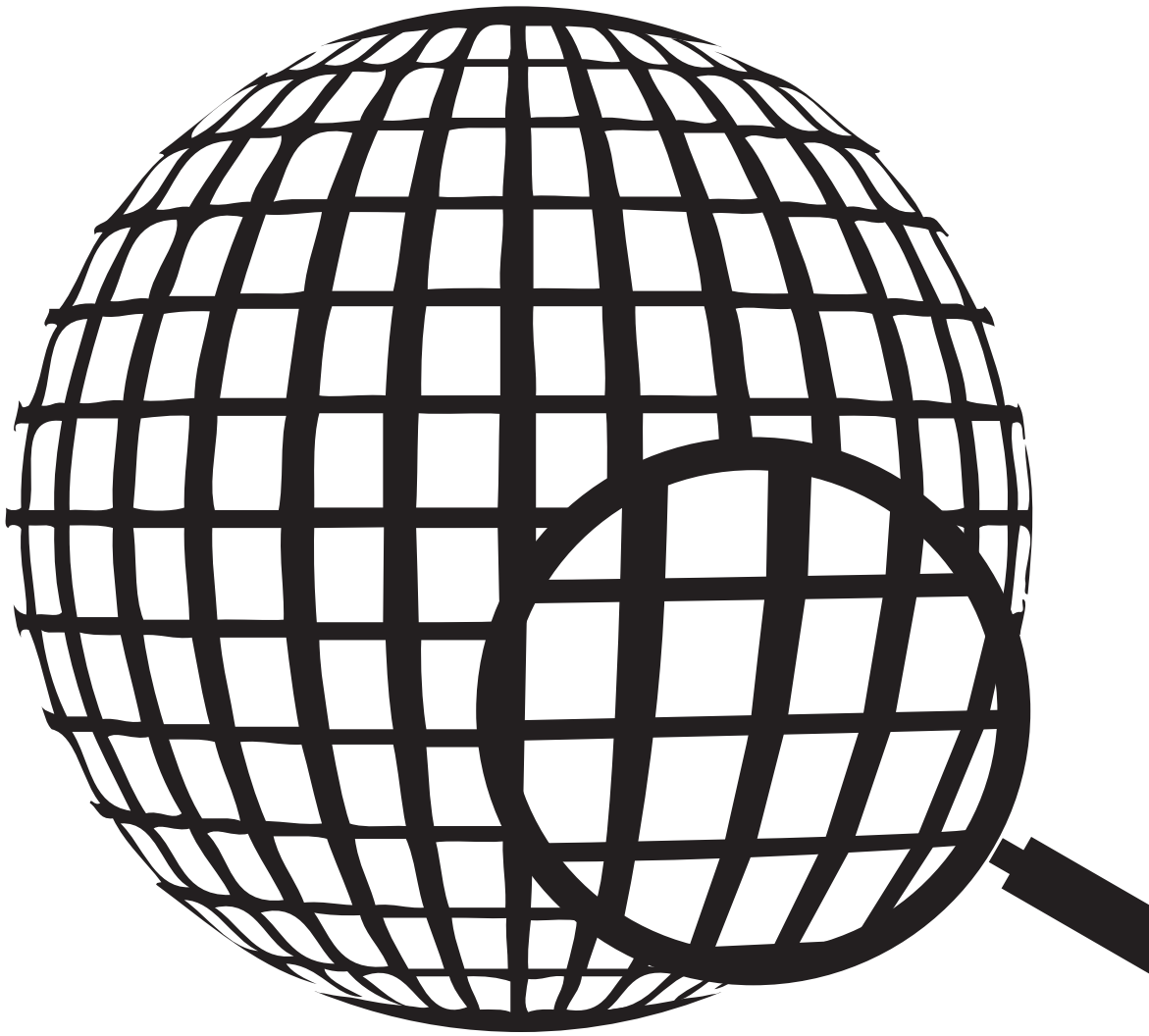
Foregenix

Foregenix Incident Response Handbook

A comprehensive guide of what to do in the unfortunate event of a compromise



Breadth of Expertise - You're in safe hands

Foregenix is a global Information Security Consultancy and Solutions Provider that is responsive to the needs of the industry and has innovation and expertise at the heart of all its activity.

With a reputation for excellence, Foregenix was established by industry veterans in 2009 and has offices in the UK, South Africa and Latin America. It offers simple, effective and strategic consultancy services as well as industry leading data security products to clients across the globe.

The highly acclaimed and respected Foregenix team has been intrinsically involved in the Payment Card Industry since the inception of the Security Standard in 2004 and has carried out thousands of PCI DSS, PA-DSS assessments, forensic investigations and penetrations tests for a variety businesses globally. Foregenix has also led the way as the world's first Qualified Security Assessor (QSA) to certify Point-to-Point Encryption (P2PE) applications and solutions.

Working to support Acquiring Banks, Service Providers, Payment Application Providers, Hosting Providers and Merchants, alongside its expanding product portfolio, Foregenix offers the following services:

- Payment Card Industry Compliance Consultancy
- Payment Card Industry Forensic Investigations
- Penetration Testing
- Mobile Application Testing
- Cardholder Data Discovery
- Managed Security Services
- Security Training

With the risk of cyber compromise a real threat to any organisation, Foregenix offers their expert advise on what to do in the unfortunate event of compromise in their Incident Response Handbook.

Have you been compromised?

When your acquiring bank (the bank who handles your credit or debit card facility) notified you that your business may have been compromised it probably came as a shock to you. Now you may feel anxious or in the dark about the events that will follow and the best course of action to take. The Foregenix Incident Response Guide is provided to answer any questions you may have about an account data compromise and the associated, processes, procedures and potential repercussions.

Firstly, it is important to appreciate that you are currently only under suspicion of being compromised and this has not yet been confirmed. This is the purpose of the forensic investigation, to ascertain if this suspicion has substance.

Account Data Compromise Confirmation – What next?

The most likely reason your bank has suggested you've been compromised is because your business was identified as a "Common Point of Purchase" (CPP). This means that the card schemes and/or bank have spotted a pattern in fraudulent card activity and identified a number of compromised cards. These cards will have been previously used within your business, typically over the previous 6 to 12 months, for legitimate payment, however subsequent to this they were used to commit fraud.

Your bank will have asked you to either appoint, or they will nominate, a PCI Forensic Investigator (PFI) to establish if you're a victim of compromise, stop the leak of sensitive information and subsequently inform you of any remedial action required in order to re-establish a secure environment for you and your customers.

What is a PFI Forensic Investigation?

Forensic Investigations are carried out in the best interest of your business. Foregenix' Forensic Investigators work in partnership with your business and react quickly to assess the cause and extent of the breach, producing a thorough report outlining the findings, listing possible vulnerabilities and providing practical advice to secure your payment card environment for the future. This ensures you minimise any future loss of sensitive data for your own business and your customers.

Immediate actions – What should I do next?

Foregenix always recommends a quick and measured response to potential compromises in order to limit the amount of possible damage. Below are a number of suggested actions to take:

1. Engage and proactively discuss all of the following steps with your commissioned forensic partner, ensuring they are suitably listed as servicing your region.
2. Do not access or modify the systems involved in the storing, processing or transmission of cardholder data - for example, do not run anti-virus, patching software, or access log files.
3. If possible, isolate and remove the suspected system(s), making sure to disable their access to and from the Internet. (It is strongly encouraged you discuss this with your Foregenix appointed forensic consultant).
4. Make a detailed log of all events, actions and consequences related to the card-processing environment and collate information surrounding all major system changes over the past 6 months i.e. software upgrades, server changes, firewall or 3rd party support changes etc.
5. Preserve any existing logs e.g. firewall, Webserver, operating systems, IDS, remote access, etc) i.e. copy these off onto backup media such as CD, DVD, USB keyfob or Drive.
6. If possible, use a fully locked-down and secure back-up system for all cardholder data management.

[1]The full list of PFI Investigators are detailed here: https://www.pcisecuritystandards.org/approved_companies_providers/pfi_companies.php

What will happen during the Investigation?

Investigations can vary depending on the extent of the compromise and most assessments may have to be conducted onsite at the location handling cardholder data. In this event a Foregenix Investigator will visit you to gather the information needed for the investigation and answer any questions you may have about the following process. It is likely the Investigator will need login credentials, as well as physical access, to your systems in order to collect the relevant information. Having your IT Administrator present is very helpful.

The Foregenix Investigator will always work efficiently and tactfully, aiming to cause as little impact upon your business as possible. Unfortunately there may be situations where disruptive issues could arise, but these will be minimised and they will work to ensure minimal business interruption. After this initial assistance, typically not much more will be required of you for the remainder of the investigation.

What does the PFI Investigator do?

The process of a Forensic Investigation can be broken down and simplified into 5 distinct phases:

1. Assessing the Situation

It is essential the Investigator fully understands the current situation and the nature of the suspected incident. They will:

a) Discuss your environment with you to understand the transaction process and flow of sensitive cardholder data

b) Discuss and review the circumstances of the investigation with you

c) Review any security remediation and precautionary steps that may have already been taken

d) Provide recommendations based on best security practice in securing your business for both yourself and your customers

e) Define the investigation scope

2. Evidence collection

The Investigator must collect evidence to assess the compromise, as a crime may have been committed and compile their forensics report against an industry provided template:

a) Foregenix will arrange the server site visit with you as soon as possible

b) The Investigator will obtain data and forensic images of all systems identified as being within the project's scope

c) The Investigator will obtain detailed network topology diagrams, system configuration settings and details of any 3rd parties providing support or services to your environment

d) It could be necessary to interview appropriate 3rd parties to further understand the environment and their role in supporting or maintaining it

3. Analysis

The Investigator will retrieve and examine all the collected evidence:

a) A full analysis of your respective system images will be completed at the Foregenix forensics laboratory to understand details of the compromise

b) A timeline of activity and the extent of the compromise should be identified

c) Any remedial actions needed to secure your business will be noted

4. Reporting

The Investigator will compile a formal report:

a) This will detail findings of the investigation, in a format acceptable by the card schemes

b) The report will cover topics such as: system and network vulnerabilities, timeframe of exposure, the entry points used by attackers, the number of exposed cards and any needed remediation

c) The Investigator will be on hand to explain any issues highlighted in the report

Typically the report will be released simultaneously to the card schemes, banks, as well as yourselves, the entity being reviewed.

Post Investigation Remediation:

Following an investigation, should the forensic report confirm that cardholder data was compromised within your environment, the card schemes and hence your acquirer will stipulate that you will be required to urgently validate your compliance to the PCI Data Security Standards (DSS) as a Level 1 organisation.

Furthermore, compromised organisations will be required to fix the vulnerabilities and high-level issues highlighted in the investigation report and your bank will require regular remediation updates. A proactive stance is strongly encouraged to ensure that your bank is kept abreast of your continued efforts in securing your own and your customer's sensitive data.

How to become PCI Compliant

As detailed above, a compromised organisation will be required to validate PCI DSS compliance as a Level 1 organisation – regardless of your transaction level.

A level 1 entity is required to do the following:

1. Engage with a Qualified Security Assessor (QSA).[2] It works best to filter on the "servicing market" for your region to ensure you're engaging with someone locally.
2. QSA to perform an on-site review of your environment
3. Authorised Scanning Vendor (ASV) to perform an external vulnerability scan
4. Regularly update your acquirer as to progress towards compliance
5. Validate compliance to the PCI DSS by working with your QSA in producing a:
    a. Report on Compliance (RoC)
    b. Attestation of Compliance (AoC)

Typically the PCI level to which an entity is validated is determined based upon the number of transactions annually. Following a breach, once the organisation has achieved compliance as a Level 1 entity, the risk should be deemed significantly reduced and as long as this is maintained, it is very likely the banks and card schemes will allow you to revert to your normal level.

The Foregenix approach to Compliance:

The above may sound daunting but the good news is that Foregenix has many years of experience in assisting and navigating through this potentially challenging process.

We appreciate your top priority is likely to be your business and your particular area of expertise, whether that is fast-food, hospitality industry, retail, e-commerce or even financial services. Data security threats can distract an organisation's focus away from their core business, often compounding the challenges being faced by the organisation.

For this exact reason, Foregenix has developed a number of packaged services, named Foregenix Security Essentials (FSE), to manage these requirements, embed security into your daily operations and allow you to get on with your business. We aim to remove the complexity of PCI Compliance, helping you to integrate best practice security policies as part of business as usual. Furthermore, security best practice for you and your customer's data will soon become mandatory under the European Data Directives and South Africa's recently formally legislated Protection of Personal Information bill.

For further information please contact Foregenix. A member of our friendly and knowledgeable team will be available to discuss any questions and even provide some free, practical and pragmatic advice.

Contact us on **+44 845 309 6232**, or **info@foregenix.com**

[2]The full list of QSAs are detailed here - https://www.pcisecuritystandards.org/approved_companies_providers/qsa_companies.php#

UK Office

8-9 High Street,
Marlborough,
SN8 1AA

UK Tel : + 4 4 (0) 8 45 309 6232
Fax : + 4 4 (0) 8 45 309 6231

South African Office

PO Box 171, River Club
2149, South Africa

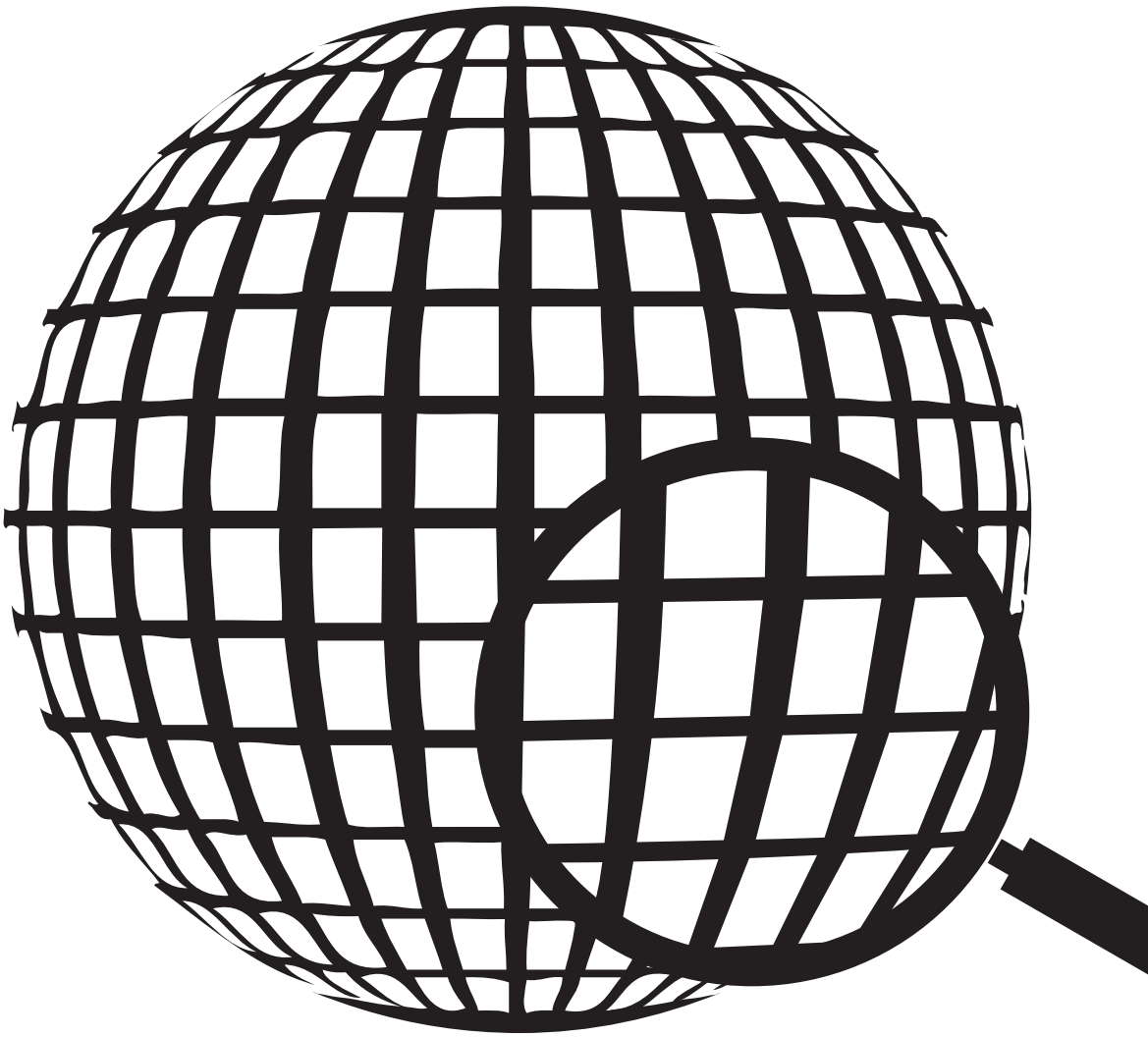
ZA Tel : +27 860 44 4461

Latin American Office

Costa Rica 1661 Of 103
11500 Montevideo
Uruguay

www.foregenix.com

Foregenix



www.foregenix.com