Payment Security Account Data Compromise (ADC)

10th July 2014

Michael Christodoulides
& Louise Hunt

All information correct at time of presentation

barclaycard

Introductions

Barclaycard has become increasingly aware that merchants may not be fully aware of devastating impacts of being a subject of a payment card account data compromise (ADC).

Barclaycard would like to take this opportunity to walk our customers through the word of Account Data Compromises and how to avoid that call...

Your conference call hosts today are Michael Christodoulides our Payment Security Manager who specialises in Third Party Risk Management and Louise Hunt a Payment Security Ecommerce Manager.

PCI Security Standards Council
PARTICIPATING ORGANIZATION

barclaycard

Agenda and Aims of Call

This call aims to provide a summary of:

- What is an Account Data Compromise (ADC)?
- What are the signs that you are at risk of an ADC (aka data security breach)?
- What should I do?
- What are my Costs, Actions and Impacts
- Is my Incident Response Plan sufficient?
- How can I reduce the risk of being a victim of a data security breach?

barclaycard

Introduction

To help set the context of this call, here is some background information:

According to a recent article in Info Security-magazine, 28% of British consumers were affected by Fraud within the past 5years.
Over a quarter of Brits have experienced card fraud in the past five years making the UK the worst offender in Europe, despite being one of the first countries to introduce chip and PIN, or 'EMV' cards nearly a decade ago.
This study augured that chip and PIN had driven fraudsters into other areas.

Source: www.infosecurity-magazine.com
http://www.infosecurity-magazine.com/view/38991/uk-worst-in-europe-for-card-fraud

barclaycard

Introduction Continued

According to The UK Card Association end of year 2013 fraud figures:
The UK is Europe's leading online shopping economy with spending by British consumers online growing by 16 per cent in 2013 to reach £91 billion.
Card payments are the main driver of this growth as they provide the most effective way to pay online.
Debit and credit cards also offer consumers protection against fraud.

Online fraud against UK retailers totalled an estimated £105.5 million in 2013, a rise of 4 per cent on the previous year.
However, there has been a substantial increase in fraud against online retailers based overseas, rising 48 per cent to an estimated £57.8 million.
Enhanced card security features, such as Chip & PIN, as well as advanced real-time fraud screening techniques employed by banks and established internet retailers, have forced criminals to change tactics.
As well as tricking customers into handing over personal and financial details (including cards and PINs), for example over the telephone while posing as officers from the bank or the police, fraudsters are also increasingly using digital attacks, such as malware and data hacks, to compromise card details.

Malware is malicious software which is unknowingly downloaded onto a computer which then enables fraudsters to steal personal or financial information or perform unauthorised actions on the device.
It is believed criminals are using these stolen details to commit fraud by targeting those online retailers which have not yet adopted security measures put in place by more established firms.

In order to help tackle this trend, experts and the police are urging consumers and online businesses to install security Software.
To prevent stolen card details being used to make purchases online, retailers are being advised to take steps to improve their security, including use of the online protection (including American Express' 'Safe Key', 'Verified by Visa' and MasterCard's 'SecureCode').

barclaycard

What is an Account Data Compromise (ADC)

Today we are going to talk about Account Data Compromises:
A compromise occurs when cardholder information taken by your business to process a payment is obtained by an unauthorised person with intent to commit fraud.

Although a compromise can affect just a small number of your customers, it can have a devastating effect on the reputation of your business. Your customers trust you to look after their cardholder data and a compromise breaks this trust.
Some well established and reputable businesses have been in the media for the substantial losses they have incurred due to fraudsters obtaining cardholder data, resulting in additional reputational damage.

Card-Not-Present (CNP) fraud accounts for 65 per cent of all card fraud, but these losses have to be seen in the context of a massive growth in CNP spending over the past ten years, especially over the internet.

The opportunity for CNP fraud takes place because merchants or their designated third parties (also known as Merchant Agents) incorrectly store cardholder data in unprotected form.
Therefore the message is clear; to reduce the risk of CNP fraud merchants and their Agents must securely protect stored cardholder data or, better still, cease storing cardholder data.
Commonly CNP fraud occurs because of vulnerabilities in online and online applications, unsecured access systems or lack of antimalware protection and poor patching policies.

However, CNP fraud can also be a result of:

✓ Theft from premises; this can occur manually or electronically.
✓ Organised Crime; you or third parties may be the victim of organised individuals within your business able to steal data.
✓ Computer Hack; insecurities in your networks or those of your third parties are exploited to steal data.

barclaycard

What are the signs that you are at risk of an ADC (aka data security breach)?

Your organisation is at risk of a data security breach if:

- It outsources to third parties but does not verify that the third party has controls in place to protect cardholder data.
- Assumes its own risk management capability is sufficiently robust to adequately protect cardholder data
- Sweats assets beyond their supported life.
- Fails to evaluate current threats (yes, even zero day) and does not apply security patches within 30 days of vendor issue.
- Pushes through systems changes without evaluating and testing the impact on the security of cardholder data.
- Operating a business model that is highly cost sensitive which leads to the "lowest cost model" of operation
- Using debugging facilities and then failing to switch off the debug logs and also fails to securely delete any cardholder data captured.
- Not resolving vulnerabilities identified in technical vulnerability scans and penetration tests.
- Failing to identify and control the scope of your cardholder data environment.
- Weak administration and control of technologies.

And these are signs that you could be at risk of a Data Security Breach.

You might have more……!

barclaycard

What increases your risk of failing to identify a breach?

The majority of security breaches are identified by an Issuer via their customers or via Card Schemes, rarely is it the merchant that self-identifies and reports.

In fact, the Verizion Data Breach Report says that 69% of breaches were spotted by an external party -9% were spotted by customers.

So what increases your risk of failing to identify a breach in cardholder data security? Here are a few thoughts:

- Not knowing the scope of your cardholder data environment (think storage, transmission processing).
- Thinking of PCI DSS solely as a point in time compliance activity rather than work that is one of continuous data security.
- Failing to correctly configure and then actively utilise logging systems that can monitor and alert "out of norm" behaviour across your network.
- Assuming it won't happen to me because.....

Source: www.verizonenterprise.com/DBIR/2014/

barclaycard

What if I discover a breach?

What if I discover a compromise?

In the event a member of staff believes that a breach may have occurred, we recommend that they report this to their line manager which in turn must be reported to your Information Security Officer. (ISO)
Once your ISO has completed their initial investigation of the suspected breach the ISO should alert management and begin in informing all relevant parties that may be affected by the compromise.
When reporting to Barclaycard you will need to:
Contact your Payment Security Risk Manager and Account Development Manager. If you do not have either of these you will need to contact our PCI team via PCI.Taskforce@barclaycard.co.uk, and mark your email urgent. This inbox is monitored daily and someone will be in contact with you to start initial conversations.
In the event this falls to a weekend or bank holiday our Customer Services department 0844 811 6666 are available and will ensure your status is reported immediately to our fraud team to make contact. You will also need to ensure that the relevant law enforcement are notified.

It is important to document a compromise response plan specific to your own business environment. If you experience or suspect a compromise you should contact Barclaycard immediately and ensure the following:

1. Ensure that no-one can access or alter compromised systems.
2. Isolate compromised systems from your network and unplug any network cables – without turning the systems off.
3. Preserve all logs and similar electronic evidence.
4. Perform a back-up of your systems to preserve their current state – this will also facilitate any subsequent investigations.
5. Log all actions you take.
6. Seek advice before you process any further transactions.
7. It is essential that you advise us of plans and changes so that we can inform the Card Schemes straight away as they look favourably when you discover and close the breach down in a timely manor.

barclaycard

What happens next?

What happens next?

When a compromise occurs, the Card Schemes insist that Barclaycard, as your acquirer, take immediate action and investigate the compromise.
Once alerted to a compromise our trained investigators will contact you as soon as possible to quickly establish how the compromise may have occurred.
They will work with you to understand your transaction flow, establish how and where your data is stored and identify any weak point in your payment transaction process.

Please inform your staff and your third parties that, in order to protect your business, our investigators require their full co-operation.
Our investigators will decide how the investigation should progress based on the level of the compromise.
They may require the involvement of a Payment Card Industry Forensic Investigator (PFI) to examine your network, hardware and software – this can take a number of weeks and could involve substantial cost to your business.

You will also need to report the theft of cardholder data to the police and obtain a crime reference.
Throughout the investigation we will provide regular updates to the Card Schemes on how the investigation is progressing.

barclaycard

What happens after the investigation?

What happens after the investigation?

As a business customer who has been compromised, your PCI status will automatically be escalated to Level 1 for 12 months. This means that you will have to pay for the services of a Qualified Security Assessor (QSA) to complete your final assessment.

If you have been storing sensitive authentication data post-authorisation, you will have 30 days from our notification to remove it and change your process and systems to eliminate post authorisation storage in the future.

You will then have to demonstrate that the following tasks have been completed within the investigators set timeframe. The timeframe given will be dependent on what type of investigation is required: (which we shall cover shortly)

- Your network perimeter is secured;
- Your payment application/process is secured; and
- Monitoring and access control is in place.

The Barclaycard Payment Security team will contact you throughout the investigation and after to help you on the road to PCI DSS compliance and meet the specific deadlines demanded by the Card Schemes.

The Barclaycard Payment Security team will require the name of the QSA you have selected and, if necessary, the Approved Scanning Vendor (ASV) to complete network vulnerability scans for you.

barclaycard

Investigation Requirements: Visa & MasterCard

So what type of investigations are there? Firstly, I shall cover Visa and there are two: Full PFI and PFI Lite.
What does PFI stand for? Payment Card Industry Forensic Investigator. They are the only personnel licensed to complete this investigation.

Full PFI: Please note this is Visa Specific:
A full forensic investigation must be carried out by a PCI SSC Approved PFI. Once a PFI investigation is complete and forensic reports submitted to the Card Schemes, a QSA (Qualified Security Assessor must then be engaged by the merchant to carry out a full RoC (Repot on Compliance) . *Many PFI companies are also QSA's so many merchants choose to use their PFI as their chosen QSA as they have understanding of the situation and status.*

Visa Expectations:
- 30days (From the Start of the PFI Investigation)- Full removal of SAD (Sensitive Authentication Data)
- 90days (This is once Visa have received the full PFI report and notified Barclaycard) of their decisions for full compliance across all payment channels.

MasterCard Expectations:
- 40days to complete the MasterCard SDP (Site Data Protection –PAT) form.
- 60 days to be fully compliant in all payment channels.

barclaycard

Investigation Requirements: Visa & MasterCard Continued

What is a PFI Lite? (Again, this is Visa specific)

This is a scaled down PCI Forensic Investigation (PFI) designed to provide acquirers and merchants with a fixed prices investigation and remediation service specifically for level 4 ecommerce merchants.
(Although we have seen this for level 3 merchants, case dependent)
Validation consists of a 40 day deadline set by Visa for the merchant to move to a PCI DSS Compliant Hosted Payment Page and to complete SAQ/A.

Should a merchant also take payments in other channels i.e. F2F/MOTO these channels will then need to be validated separately within given timescales by Barclaycard.
Please note, if these channels are applicable, Barclaycard require these specific channels to be validated via an SAQ signed by a QSA.

Please note: If PFI Lite has been approved by Visa Europe, please note that this will not cover MasterCard and separate requirements may still apply.
Both Schemes issue deadlines to Barclaycard independently, therefore it is imperative that your business works to validate full compliance immediately.

barclaycard

You need to budget.

What is the cost of a data breach? –How long is a piece of string…

It will always be more than you want it to be. Your unbudgeted costs will vary, depending on the nature and scale of the breach.

Your budget line items will need to include:

- PFI investigation
- Remediation
- Verification of Compliance (QSA)
- Achieving compliance with the standard
- Undisclosed financial penalties for failing to maintain Payment Security

And then there are other factors to consider (lost opportunity costs)

- Business Impact
- Brand Reputation
- Loss of customer trust
- Re-prioritisation of other internal business projects
- Potential slow down in growth due to re-deployment of resources to contain and remediate a security breach.

Example! We have experience of the positive side of self-reporting, whereby the merchant, took relevant action to inform and contain and remediate the breach immediately reducing the adverse impact to themselves and their Customers.

barclaycard

Top Tips & Incident Response Plan

We have covered the aspects of what to do in the event of a breach, how to report and the consequences of a breach. We would now like to look at a more proactive approach to this and how to mitigate the impact of a breach.

What should this entail?

Requirement 12.10. (V3) of the standard requires an incident response plan to be implemented in preparation to respond immediately to a system breach, as laid out in requirement 12.10.1 A&B:

1. Roles, responsibilities and communication and contact strategies in the event of a compromise including notification of the payment brands, at a minimum?
2. Specific incident response procedures?
3. Business recovery and continuity procedures?
4. Data Backup processes?
5. Analysis of legal requirements for reporting compromises?
6. Coverage and responses of all critical system components?
7. Reference or inclusion of incident response procedures from the payment brands?

12.10.3 to 12.10.6 also covers incident response, testing, alert procedures and expected testing to ensure this is in place.

Top Tips & Incident Response Plan Contin..

If that's not enough for you, NIST have an in-depth guidance incident response which includes:

- Create an incident response policy and plan
- Develop procedures for performing incident handling and reporting
- Set guidelines for communicating with outside parties regarding incidents
- Select a team structure and staffing model
- Establish relationships and lines of communication between the incident response team and other groups, both internal (e.g., legal department) and external (e.g., law enforcement agencies, PFI, Acquirer etc.)
- Determine what services the incident response team should provide
- Staff and train your incident response team.

Currently within Europe we don't have mandatory breach notification, so our advice would always be to consult with Barclaycard and wait for the PFI/PFI Lite to both close the breach and accurately report the numbers of cards at risk before making public announcements.

To summarise responding to outside parties you need a:

- Command and Control
- Single media person and channel
- Use Social Media effectively
- Inform
- Assure and remediate.

barclaycard

How can I reduce the risk of being a victim of a Data Security Breach?

We have put together some guidelines to help you minimise your risk of compromise. It's not exhaustive but will go a long way to help you.

1. Maintain your PCI DSS compliant status – this is the best way to minimise your risk of cardholder data compromise. Compliance must be renewed every year and this involves completing a Self Assessment Questionnaire (SAQ) or onsite audit. You may also have to continue performing and passing quarterly network vulnerability scans depending on your PCI level. To find out which level you bu visiting the Visa website or visit our Barclaycard website for this matrix

2. Ensure that any third parties you use are PCI DSS compliant and registered with Visa at www.visamerchantagents.com. These may include Payment Service Providers, fulfilment houses, bureau services and internet hosting companies.

3. If you are a Level 3 merchant and are using our Data Security Manager portal you have access to our dedicated helpdesk team via 0844 811 0089 or using the Live Chat facility. Our call agents are available to provide you with assistance on ways in which your business can lower the risk.

4. If you process payments using a computer, make sure you have firewall and antimalware software in place which is up to date.

5. If you have purchased software which uses a password, make sure you change the password, and only the members of staff who requires access to the software will be given the password. - Use strong passwords

6. Train staff on required PCI DSS procedures (e.g. cardholder data security and retention) and create a security policy for all to follow if you don't already have one.

7. Ensure coders are trained in secure-coding practice (i.e OWASP & vendor specific training)

barclaycard

Continued

8. Conduct Payment Security testing prior to implementation

9. Implement Secure Code on your website

10. Configure and use logs correctly. Switch off de-bugging logs.

11. Patch, Patch and Patch!! (Zero days always happen, but at least mitigate known risks!)

12. Remove card security data and limit data retention.

13. Protect the data network (e.g. LANs, WANs).

14. Secure any application handling cardholder data.

15. Protect your environment through monitoring and access control.

16. Securely protect remaining cardholder data (card number and expiry date) using techniques such as encryption or Tokenisation

17. Verify your 3rd Parties Payment Security Capability.

barclaycard

How do I find out more about ADC's?

Useful tools and information to increase your understanding and knowledge about ADC's

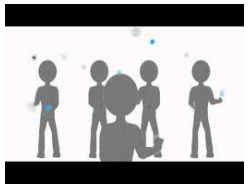
- Barclaycard Payment Security Leaflets
- Our website at www.barclaycard.co.uk/pcidss
- Barclaycard ADC Case Studies: http://www.barclaycard.co.uk/business/accepting-payments/payment-security/pci-dss/how-do-i-become-compliant
- SSC at www.pcisecuritystandards.org
- Videos on our DSM portal www.barclaycarddatasecuritymanager.co.uk
- Verizon Data Breach Report 2014 www.verizonenterprise.com
- OWASP (Open Web Application Security Project) www.owasp.org
- SANS (System Admin & Network Security) www.SANS.org
- VISA –What to do if compromised? White Paper www.visa.com/merchants/whattodoifcompromised
- ICO Information Security Report www.infosecurity-magazine.com
- UK Financial Fraud Bureaux
- UK Card Association www.theukcardassociation.org.uk

barclaycard

Find us on

LinkedIn

Barclaycard Business Solutions Payment Security



www.youtube.com/watch?v=-ngt2buzI7Y

www.youtube.com/watch?v=ucwDxTa-RLI

barclaycard

Awards and credentials

Elected Board member of the Payment Card Industry Security Standards Council (PCI SSC)

Winner of FSTech Awards Compliance Project of the Year 2013

Winner of FSTech Awards Anti-Fraud/Security Strategy of the Year 2013

Winner of Data Security Award , MPE Awards 2012

Winner of Merchant Award, MPE Awards 2012

Winner of Information Security Team of the Year, SC Magazine Europe Awards 2012

Winner of Information Security Team of the Year, SC Magazine Europe Awards 2011

Winner of the Data Security Award, European Card Acquiring Forum (ECAF) Awards 2010

SC MAGAZINE AWARDS 2012 EUROPE WINNER

PCI Security Standards Council™ PARTICIPATING ORGANIZATION

FStech awards 2013 WINNER

FStech awards 2014 SHORTLISTED

barclaycard