

e-finance&payments law&policy

FEATURED ARTICLE

Volume 3, Issue 3, March 2009



cecile park publishing

Head Office UK: Cecile Park Publishing Limited, 17 The Timber Yard, Drysdale Street, London N1 6ND
tel: +44 (0)20 7012 1380 fax: +44 (0)20 7729 6093 info@e-comlaw.com
www.e-comlaw.com

Data Protection: Analysis: Heartland security breach

Heartland Payment Systems – a credit card processing company in the US – announced recently that a data breach had occurred, compromising a minimum of 500 banks and an undetermined number of cards. Geoff Webb, Senior Manager of Marketing at NetIQ Corporation discusses what organisations can learn from the breach and examines what organisations can do to prevent similar breaches from arising.

'..it was the age of wisdom, it was the age of foolishness..'

Charles Dickens,
A Tale of Two Cities

Introduction

Despite the incredible investment governments and private companies have made in security technologies, both the frequency and the scale of reported data breaches are increasing explosively. The number of compliance mandates that must be met is at an all-time high, yet the security value of practices they demand is being called sharply into question by the failure of organizations to protect sensitive information. From a data security perspective it is the best, and worst, of times.

For context, I'm going to look at two very different breaches, and try to draw some parallels that may apply to your organization. In many ways, what makes these different – and they are very different – is just as important as what they have in common.

The two I will look at are the Heartland Payment Systems Breach, now being dubbed as the largest in history and the recent breach at the Federal Aviation Administration (FAA), which while much smaller, provides some disturbing insights into the future of that rarest commodity - private information.

Background to Heartland Payment Systems and FAA

These two breaches both occurred in the United States within the last twelve months and have been widely reported on in the United States. There was nothing about either breach that would not apply equally to organizations from the United Kingdom, or indeed anywhere in the world.

If you missed the news stories, here are the key facts, at least as they are publically available now:

Heartland Payment Systems breach

Heartland Payment Systems is one of the largest credit card processing companies in the US and by its own

estimates, processes upwards of 100 million transactions per month. In January 2009, Heartland announced that a breach had occurred sometime in the previous year and that, for an undetermined amount of time, someone had access to an extensive amount of credit card information through some well-placed malware code. As of the time of writing, the scope of this breach is still being determined, but at a minimum, over 500 banks have reportedly been affected. While the number of compromised cards is not known, clearly an extended breach involving such a large number of transactions per month is likely to have a significant impact.

FAA breach

The FAA breach appears to be a very different animal. The stolen information was taken, it seems, from an old system apparently being used as a test-bed for application developers. In what appears to be an opportunistic attack, external hackers stumbled upon the relatively poorly protected system and made off with sensitive files. Unfortunately, one of the files stolen contained personal information dating back to 2006 on some 45,000 current and former employees.

Similarities and differences

The two breaches were similar in that sensitive information was stolen from what should have been secured infrastructure. In the case of the FAA, the organization as a whole was considered so secure that it was actually used as an example of what to do right within the US Federal Government. Yet the breach occurred and data was stolen.

In both cases, information was stolen out from under the very noses of competent and active security teams. Additionally, external assessments of the security protecting their

information had shown them to be at the very least, as good as their peers.

They differed, however, in a highly significant way. It seems likely that the FAA breach was the result of an (un)lucky find on the part of hackers (external parties). In the case of Heartland, however, it is almost certain that highly competent and financially motivated attackers worked from within. They placed custom malware designed to sniff credit card information at a weak point in the processor's network. This kind of internal attack is becoming increasingly common, and is causing considerable concern in the financial sector and the security industry in general.

Fundamentally, these two breaches have some important lessons to teach about the nature of data, and how organizations of all kinds, commercial, private and public, handle it. Most significantly they are clear indicators that something has gone terribly wrong, not only in the way we secure data but in the very way we think of information protection within and beyond corporate walls.

What we can learn

Despite getting breached, both organizations did some things right and we can learn much from their respective responses to the events.

Both organizations moved quickly to notify those who may have been affected by the data breaches, and are now focusing on eliminating the problem in the future. Although both organizations have received considerable criticism for the breaches, it's fair to say that it might have been far worse had they not moved more rapidly.

One of the more interesting lessons of the FAA breach is that data is sticky and difficult to find - one recent study showed that 66 % of breaches that occur involve data that organizations did not know even existed. FAA information that was old, yet still sensitive in nature, turned up in a very surprising location.

Once information exists in electronic form, it can be difficult to track and therefore equally difficult to secure. This will become especially challenging as organizations embrace more aggressive virtualization strategies, where not only the data but the actual server itself exists as an electronic image that is easy to reproduce.

Clearly, sensitive information exists long after its utility has expired – a chilling thought when we consider the difficulty organizations apparently have in keeping it secure.

A significant failure in configuration control was likely at the root of the problem for Heartland. Unmanaged change is the bane of good security. Configuration control is everything – stopping malware, (unauthorized and harmful software), or changes that weaken security, is only possible once good controls are in place to detect changes as they occur, and enforce security policies. What organizations need, then, is to implement a strong change management process.

One fact that organizations must come to grips with is that compliance is not going to make you secure – Heartland and the PCI DSS are perfect examples of this. Whether Heartland was compliant at the time of the breach or not is yet to be determined, but they were certainly compliant at some point and the reality is that any certificate of compliance is such a narrow snapshot as to be almost meaningless from a data security perspective.

Some next steps

While these two breaches are already in the past, there are some very timely lessons that can be drawn from what happened and applied to security programs immediately to establish a proper security posture and hopefully prevent any loss of critical data. Here are some basic first steps that organizations like yours can take to help prevent similar breaches from arising:

- Start to think of data differently – you can't secure it if you can't find it.
- Implement change controls detecting and managing change and tying changes to your ticketing/configuration management system, is the only way you can have any chance of securing critical systems.
- Look long and hard at how you monitor administrator/privileged user activity - these are your single greatest threat. Yes, attacks come from outside, but they are likely to be far, far less damaging than breaches originating inside. While there is no direct evidence of insider involvement in the Heartland breach, similar breaches have often involved privileged access to a

system, enabling internal placement of the malware. Privileged users may not always be employees – contractors and even trusted partners may represent every bit as much of a threat.

- Have a plan for breach response - know what a breach looks like, and know how to respond if and when one occurs. Identify who to call and how to notify customers.
- Think about ways to reduce the workload on your security teams the reality is that breaches oftentimes would be detectable if only the teams involved had been able to spend the time to review the information already being collected.

The Heartland and FAA breaches are both perfect examples of how organizations with good security practices can remain vulnerable, either to a persistent, skilled attacker or sometimes simple bad luck. Reducing the time between an attempted attack and a response is essential to reduce the scope of a breach and minimize the subsequent damage a successful attack causes.

By combining change control best practices with a new perspective on compliance and security process automation, organizations like yours, Heartland and the FAA can reduce risk and narrow the window of exposure. This will enable effective protection of corporate good names and more importantly, our collective private information.

Geoff Webb

Senior Manager of Marketing
NetIQ Corporation
geoff.webb@netiq.com

Melissa Lang

Voce Communications for NetIQ
mlang@vocecomm.com

This electronic transmission contains confidential information intended only for the person(s) named. Any use, distribution,

copying, or disclosure by any other person is strictly prohibited. If you received this transmission in error, please notify the sender by return e-mail and delete all copies of this message.



cecile park publishing

Head Office UK: Cecile Park Publishing Limited, 17 The Timber Yard, Drysdale Street, London N1 6ND
tel +44 (0)20 7012 1350 fax +44 (0)20 7729 6093 info@e-comlaw.com
www.e-comlaw.com

Registered number 227876 Registered address 141 Waterloo Street, London W6 0UT VAT registration 57783903

e-commerce law & policy

Many leading companies, including Amazon, BT, eBay, FSA, Orange, Vodafone, Standard Life, and Microsoft have subscribed to ECLP to aid them in solving the business and legal issues they face online. ECLP was nominated in 2000 and again in 2004 for the British & Irish Association of Law Librarians' Legal Publication of the Year. **A twelve month subscription is £420 (overseas £440) for twelve issues and includes single user access to our online database.**

e-commerce law reports

You can now find in one place all the key cases, with analysis and comment, that affect online, mobile and interactive business. ECLR tracks cases and regulatory adjudications from around the world. Leading organisations, including Clifford Chance, Herbert Smith, Baker & McKenzie, Hammonds, Coudert Brothers, Orange and Royal Mail are subscribers. **A twelve month subscription is £420 (overseas £440) for six issues and includes single user access to our online database.**

data protection law & policy

You can now find in one place the most practical analysis, and advice, on how to address the many problems - and some opportunities - thrown up by data protection and freedom of information legislation. DPLP's monthly reports update an online archive, which is an invaluable research tool for all those who are involved in data protection. Data acquisition, SMS marketing, subject access, Freedom of Information, data retention, use of CCTV, data sharing and data transfer abroad are all subjects that have featured recently. Leading organisations, including the Office of the Information Commissioner, Allen & Overy, Hammonds, Lovells, BT, Orange, West Berkshire Council, McCann Fitzgerald, Devon County Council and Experian are subscribers. **A twelve month subscription is £390 (public sector £285, overseas £410) for twelve issues and includes single user access to our online database.**

world online gambling law report

You can now find in one place analysis of the key legal, financial and regulatory issues facing all those involved in online gambling and practical advice on how to address them. The monthly reports update an online archive, which is an invaluable research tool for all those involved in online gambling. Poker, payment systems, white labelling, jurisdiction, betting exchanges, regulation, testing, interactive TV and mobile gaming are all subjects that have featured in WOGLR recently. Leading organisations, including Ladbrokes, William Hill, Coral, Sportingbet, Betyle, DGMS, PMU, Orange and Clifford Chance are subscribers. **A twelve month subscription is £520 (overseas £540) for twelve issues and includes single user access to our online database.**

world sports law report

WSLR tracks the latest developments from insolvency rules in football, to EU Competition policy on the sale of media rights, to doping and probity. The monthly reports update an online archive, which is an invaluable research tool for all involved in sport. Database rights, sponsorship, guerrilla marketing, the Court of Arbitration in Sport, sports agents, image rights, jurisdiction, domain names, ticketing and privacy are subjects that have featured in WSLR recently. Leading organisations, including the England & Wales Cricket Board, the British Horse Board, Hammonds, Redgate Fielder, Clarke Wilmott and Skadden Arps Meszger & Flom are subscribers. **A twelve month subscription is £520 (overseas £540) for twelve issues and includes single user access to our online database.**

priority order form

FAX +44 (0)20 7729 6093
CALL +44 (0)20 7012 1350
EMAIL dan.towers@e-comlaw.com
ONLINE www.e-comlaw.com
POST Cecile Park Publishing 17 The Timber Yard, Drysdale Street, London N1 6ND

- Please enrol me as a subscriber to **e-commerce law & policy** at £420 (overseas £440)
- Please enrol me as a subscriber to **e-commerce law reports** at £420 (overseas £440)
- Please enrol me as a subscriber to **data protection law & policy** at £390 (public sector £285, overseas £410)
- Please enrol me as a subscriber to **world online gambling law report** at £520 (overseas £540)
- Please enrol me as a subscriber to **world sports law report** at £520 (overseas £540)

All subscriptions last for one year. You will be contacted at the end of that period to renew your subscription.

Name	<input type="text"/>		
Job Title	<input type="text"/>		
Department	<input type="text"/>	Company	<input type="text"/>
Address	<input type="text"/>		
Address	<input type="text"/>		
City	<input type="text"/>	State	<input type="text"/>
Country	<input type="text"/>	Postcode	<input type="text"/>
Telephone	<input type="text"/>	Fax	<input type="text"/>
Email	<input type="text"/>		

1 Please **invoice me** Purchase order number
Signature Date

2 I enclose a **cheque** for the amount of
made payable to 'Cecile Park Publishing Limited'

3 Please debit my **credit card** VISA MASTERCARD
Card No. Expiry Date
Signature Date
VAT No. (if ordering from an EC country)

Periodically we may allow companies, whose products or services might be of interest, to send you information. Please tick here if you would like to hear from other companies about products or services that may add value to your subscription.