VIEIRA DE ALMEIDA
& Associados Sociedade de Advogados, R.L.

03.04.2008

Data Security e Protecção Jurídica

- Abordagem jurídica ao PCI *Compliance* -

O que nos deve preocupar…

- Em Fevereiro de 2005, o **Bank of America** reclamou a perda de mais de **1,2 milhões de registos** dos seus clientes.

- Em Junho de 2005, a **CardSystems** foi processada numa série de casos por ter alegadamente falhado na protecção de dados pessoais de **40 milhões de clientes**.

- Em Janeiro de 2007, a **Moneygram**, confirmou que o servidor da empresa foi indevidamente acedido através da Internet o qual continha cerca de **79.000 contas de clientes** (incluindo nomes, moradas, números de telefones e em alguns casos, os números das contas bancárias)

- **TJX Companies Inc.** divulgou publicamente que tinham sofrido uma intrusão/ataque não autorizada no seu sistema electrónico dos cartões de crédito/débito teve uma falha de segurança numa das lojas do grupo e foi, por isso, responsável pela perda de dados relativos a 45,7 milhões de contas de clientes no espaço de dois anos.

O que nos deve preocupar…

Hannaford sofreu um ataque aos seus computadores, do qual resultou o **roubo** de **4,2 milhões** de dados de **cartões bancários de clientes**

"Nos próximos anos, 20% a 30% dos grandes grupos internacionais poderão incorrer em custos que podem variar entre $5-$20 milhões (i.e. aproximadamente entre € 4 000 000 e € 17 000 000) em virtude do incumprimento das regras de protecção de dados pessoais."

“Data Security” e enquadramento jurídico

- “Auto-regulação” (regras/directivas do PCI-DSS)
- Legislação relativa ao Sector Bancário (**Sigilo Bancário** (RGICSF e Regime Jurídico dos contratos à distância relativos a serviços financeiros celebrados com consumidores*)
- Legislação de **Dados Pessoais** Geral e do Sector das Comunicações Electrónicas
- …

PCI-DSS

- ✓ O **PCI-DSS** são regras de segurança para protecção de dados de cartão de crédito

PCI-DSS

- ✓ O PCI está divido em 12 "*security requirements* ("Digital Dozen") que estão organizados em 6 categorias:

  - Criar e manter uma rede segura (*firewalls*, etc)
  - Proteger a informação do titular do cartão (encriptar os dados..)
  - Dispor de um sistema de gestão da vulnerabilidade (utilizar antivírus aplicações seguras)
  - Implementar medidas restritas de acesso à informação (*business need-to-know*)
  - Monitorizar e testar a rede e a informação (testar regularmente os níveis de segurança)
  - Dispor de uma política de segurança da informação (aplicável a funcionários e prestadores de serviços)

Sector bancário

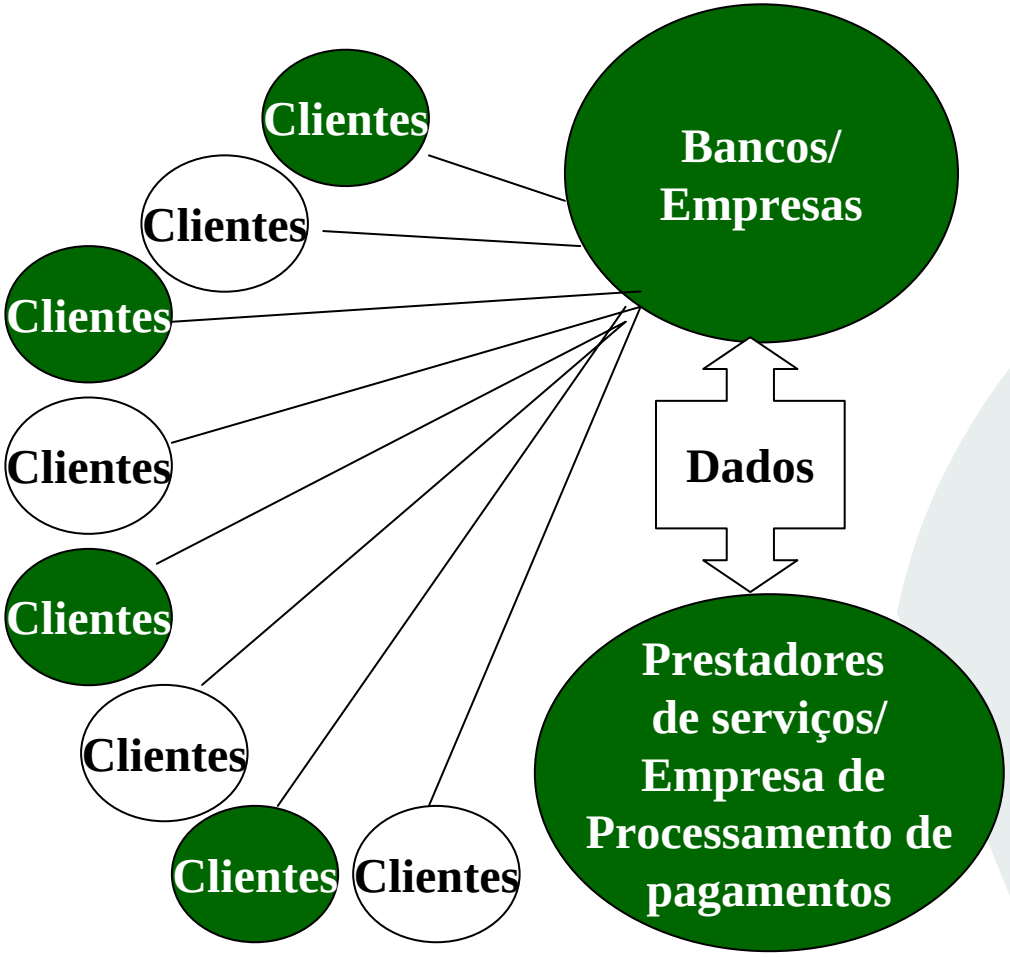
- ✓ Nos casos de pagamento por pagamento por cartão:
  - ➢ deve ser garantida consumidor o direito de anular um pagamento em caso de utilização fraudulenta do seu cartão
  - ➢ No caso de utilização fraudulenta, as quantias devem ser creditadas ou restituídas ao consumidor
  - ➢ O dever de restituição não prejudica o direito de regresso da entidade emissora ou gestora do cartão electrónico contra os autores/responsáveis pela fraude

Sector bancário

✓ O que é que está sujeito a **segredo bancário**?

"*Estão designadamente sujeitos a segredo os* ***nomes dos clientes***, ***as contas*** *de depósito e os seus* ***movimentos*** *e outras operações bancárias*" (Artigo 78.º do RGICSF).

Protecção de dados pessoais



Todas as **transacções** (informações relativas a pagamentos) e **recolha de dados pessoais** dos clientes

Protecção de dados pessoais

O que são Dados Pessoais ?

Todo ou qualquer tipo de informação em qualquer tipo de suporte (e.g. informático, papel, som, imagem)

Referente a uma pessoa singular (titular dos dados)

Identificada ou Identificável

e.g. nome, morada, endereço electrónico, fotografias, etc.

e.g. n.º do BI, endereço IP *(Internet Protocol)*, etc.

O que é o tratamento de dados pessoais ?

Qualquer tipo de operação que incida sobre dados pessoais utilizando ou não meios automatizados

Recolha, registo, organização, conservação, adaptação, alteração, recuperação, consulta, utilização, comunicação por transmissão, difusão ou qualquer outra forma de colocação à disposição, com comparação ou interconexão, bloqueio, apagamento ou destruição.

Protecção de dados pessoais

- ✓ O tipo de dados determina as formalidades a cumprir

Quem é o responsável pelo tratamento ?

Qualquer pessoa, singular ou colectiva, que individualmente ou em conjunto com outrem determine as finalidades e os meios de tratamento dos dados pessoais.

Quem é o subcontratante ?

A pessoa singular ou colectiva, a autoridade pública, o serviço ou qualquer outro organismo que trate os dados pessoais por conta do responsável pelo tratamento.

Protecção de dados pessoais

- ✓ O que deve assegurar o responsável pelo tratamto
  - Direito de informação
  - Direito de Acesso
  - Direito de oposição
  - Actualização de dados
  - Legalização do tratamento dos dados
  - **Segurança**
  - **Confidencialidade**
  - ….

Protecção de dados pessoais

- ✓ Adoptar **medidas de segurança** para protecção de dados da empresa, como:
  - ➢ Controlo da entrada nas instalações
  - ➢ Controlo dos suportes de dados
  - ➢ Controlo da inserção
  - ➢ Controlo de utilização
  - ➢ Controlo de acesso
  - ➢ Controlo da transmissão e do transporte
  - ➢ Controlo da introdução

Protecção de dados pessoais

- Todos aqueles que oferecem **redes** e **serviços** de **comunicações electrónicas** devem :

  - colaborar entre si no sentido da adopção de **medidas técnicas** e **organizacionais eficazes** para garantir a **segurança dos seus serviços** e, se necessário, **a segurança** da própria **rede**

Essas medidas devem ser **adequadas à prevenção dos riscos existentes**, tendo em conta a proporcionalidade dos custos da sua aplicação e o estado da evolução tecnológica

Protecção de dados pessoais

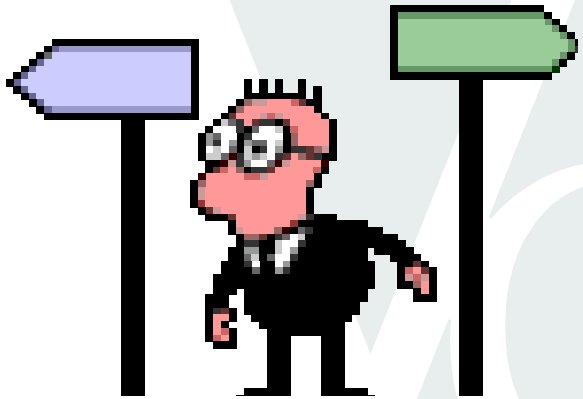
- As **empresas** que oferecem **redes e ou serviços de comunicações electrónicas** devem garantir a **inviolabilidade das comunicações** e respectivos **dados de tráfego** realizadas através de **redes públicas** de comunicações e de **serviços de comunicações electrónicas** acessíveis ao **público**.

Em caso de **risco** especial de **violação da segurança da rede**, as empresas que oferecem serviços de comunicações electrónicas acessíveis ao público devem **gratuitamente** informar **os assinantes** desse serviço da **existência** daquele **risco**, bem como das **soluções** possíveis para o **evitar e custos** prováveis das mesmas

A violação das regras

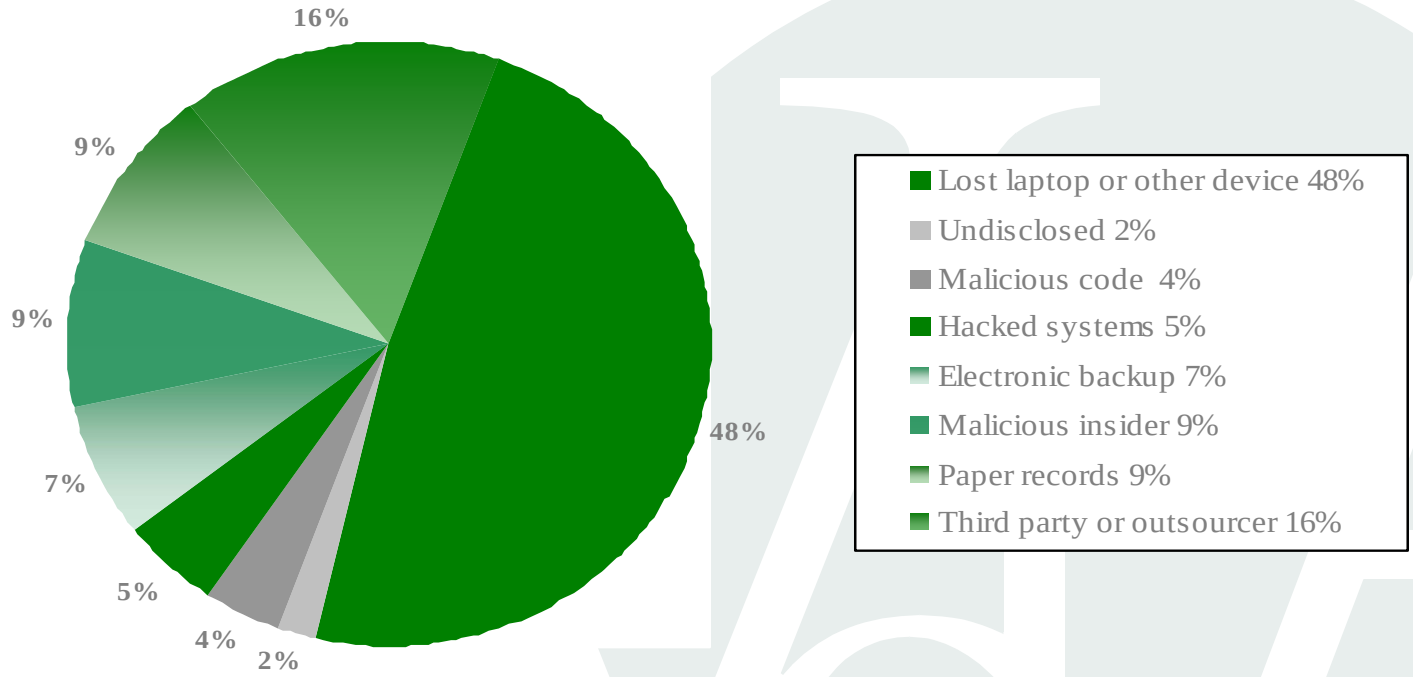
- Responsabilidade civil pelos prejuízos causados.
- Responsabilidade criminal (pena de prisão até 2 anos ou pena de multa até 240 dias).
- Responsabilidade contra-ordenacional (coimas até € 30.000,00 ou 5.000.000,00).
- Sanções acessórias (proibição temporária ou definitiva de tratamento, bloqueio, apagamento ou destruição dos dados; publicidade da sentença).

Boas práticas para evitar "data breach"



Evitar *Data Security Breaches*

- A protecção dos sistemas de informação implica que se olhe para toda a cadeia de circulação da informação



Evitar *Data Security Breachs*

- ✓ Realizar uma **auditoria aos processos de tratamento dados** existentes na empresa

- ✓ Promover uma **gestão centralizada** das processamento de dados existentes na empresa/nomear um "***Data Privacy Officer***" ou ***"Data Security Officer"***

- ✓ Definir uma **política de tratamento** de dados pessoais

- ✓ Adoptar um **Regulamento de Segurança da informação**

Evitar *Data Security Breachs*

- ✓ Dar **formação** aos **funcionários da empresa** para garantir a segurança dos dados

- ✓ Adoptar **medidas de segurança** para protecção de dados da empresa

….e ter uma estratégia de "***Damage Control***" em caso de *data security breach*

A Message from Hannaford CEO Ron Hodge

"Dear Customer:

Hannaford has contained a **data intrusion** into its computer network that resulted in the theft of customer credit and debit card numbers. (…)
We sincerely regret this intrusion into our systems, which we believe, are among the strongest in the industry. The **stolen data** was limited to **credit and debit card numbers** and expiration dates, and was **illegally accessed** from our computer systems during transmission of card authorization. (…) We realize this **incident** may **raise concerns** and **questions** for our **customers** (…)."

MUITO OBRIGADA

Aviso:

Este documento destina-se única e exclusivamente a servir de suporte à apresentação no seminário "PCI Compliance Event" organizado pela CISCO, pelo que se encontra vedada a sua cópia ou circulação. As informações e opiniões expressas neste documento e na apresentação efectuada são de carácter geral, não substituindo o recurso a aconselhamento jurídico especifico.