



# USANDO INTELIGÊNCIA NO COMBATE A FRAUDES NO COMÉRCIO ELETRÔNICO

Walter Hannemann, Diretor  
[walter@ciashop.com.br](mailto:walter@ciashop.com.br)

# USANDO INTELIGÊNCIA NO COMBATE A FRAUDES NO COMÉRCIO ELETRÔNICO

- Fraudes nos Negócios Eletrônicos
  - ✓ qual é o risco
  - ✓ como é a fraude
  - ✓ prevenção é a solução
  - ✓ análise de risco hoje
  - ✓ o futuro

# USANDO INTELIGÊNCIA NO COMBATE A FRAUDES NO COMÉRCIO ELETRÔNICO

## Qual é o risco?

- Medidas técnicas de segurança não tem efeito – confusão conceitual
- 3% de perdas diretas com fraudes no Brasil
- Anos de investimento em prevenção = 1% de perdas diretas nos EUA
- Para cada fraude, 3 a 4 pedidos rejeitados
- Custo total = perda direta + bons pedidos rejeitados + custo da administração do risco

# USANDO INTELIGÊNCIA NO COMBATE A FRAUDES NO COMÉRCIO ELETRÔNICO

## Como acontece a fraude

- Fraudador usa cartão alheio comprometido; verdadeiro dono do cartão não reconhece o débito; administradora ou banco ordena o “charge back”
- Comprometimento (clonagem): 96% no mundo físico, 2% Internet
- Por contrato, risco é do lojista
- Charge back pode ocorrer até 1 ano após a transação

# USANDO INTELIGÊNCIA NO COMBATE A FRAUDES NO COMÉRCIO ELETRÔNICO

## Como acontece a fraude



# USANDO INTELIGÊNCIA NO COMBATE A FRAUDES NO COMÉRCIO ELETRÔNICO

## Prevenção

- A prevenção passa obrigatoriamente por autenticar o comprador
- É impossível ou inviável a recuperação da perda
- Deve-se evitar o inconveniente do contato direto com o comprador

Como então tomar a decisão de envio ou não dos produtos?

- Análise do pedido para identificar características típicas
- Cruzamento de informações com bases de dados confiáveis
- Processo deve ser rápido

# USANDO INTELIGÊNCIA NO COMBATE A FRAUDES NO COMÉRCIO ELETRÔNICO

## Prevenção

- Revisão manual é o método mais utilizado, com alta incidência de contato com o cliente (78% EUA, 83% Brasil)
- Após identificado pedido de risco, dados do pedido são cruzados com bases de dados externas
- Processo manual difícil, demorado e caro
- Quantas transações podem ser checadas por dia? Com que estrutura e com que nível de acerto?

# USANDO INTELIGÊNCIA NO COMBATE A FRAUDES NO COMÉRCIO ELETRÔNICO

## Análise de Risco

- Já que não é possível verificar todos os pedidos, devo concentrar esforços nas transações de risco mais elevado
- Como fazer a pontuação de risco?
  - Pré-requisitos:
    - Conhecimento profundo do negócio e dos perfis de fraude
    - Bancos de dados de transações
    - Sistema integrado inteligente

# USANDO INTELIGÊNCIA NO COMBATE A FRAUDES NO COMÉRCIO ELETRÔNICO

## Análise de Risco

- Componentes básicos da análise de risco:
  - Regras de negócio: verificação e pontuação de itens críticos  
Exemplos:  
Estatística: um pedido com valor de 3X o ticket médio tem 3,4X mais chance de ser fraude.  
Pedidos com múltiplos produtos de um mesmo tipo, endereço de entrega diferente do endereço de cadastro  
  
O óbvio: separar esses pedidos para checagem.

# USANDO INTELIGÊNCIA NO COMBATE A FRAUDES NO COMÉRCIO ELETRÔNICO

## Análise de Risco

- Componentes básicos da análise de risco:
  - Listas Negras
    - Deve listar dados da fraude e não cadastros de compradores
    - Informações relevantes na fraude: dados da entrega, e-mail
  - Listas Brancas
    - Informa o perfil e o histórico de compras para análise de comportamento
    - Deve ter uma responsável política de privacidade

# USANDO INTELIGÊNCIA NO COMBATE A FRAUDES NO COMÉRCIO ELETRÔNICO

## Análise de Risco

- Componentes básicos da análise de risco:
  - Inteligência Artificial - Rede neural
    - Simula o pensamento de um especialista humano, mas com maior precisão, velocidade e consistência
    - Permite um constante “aprendizado”
    - Devolve uma pontuação de risco (geralmente de 0 a 1000)

# USANDO INTELIGÊNCIA NO COMBATE A FRAUDES NO COMÉRCIO ELETRÔNICO

## Análise de Risco

- Sistema integrado de análise de risco: a inteligência aplicada na solução do problema
  - Objetivo: separar os bons pedidos daqueles que precisam “autenticação”.
  - Utiliza os componentes básicos de forma integrada para otimizar os resultados
  - Na identificação de pedidos de risco elevado, automatiza ou facilita o acesso à ferramentas de autenticação ou contato com o cliente

# USANDO INTELIGÊNCIA NO COMBATE A FRAUDES NO COMÉRCIO ELETRÔNICO

## Análise de Risco

- Sistema integrado de análise de risco: a inteligência aplicada na solução do problema
  - Através de regras ajustáveis, define o “ponto de corte”.

Se em 1000 pedidos diários é viável “autenticar” 250, então quero que somente os 250 de maior risco sejam analisados. Se posso analisar apenas 100, ajusto as regras para que somente os 100 de maior risco sejam separados para revisão.
  - Permite o acompanhamento e a realimentação de todas as transações passadas – aprendizado contínuo

# USANDO INTELIGÊNCIA NO COMBATE A FRAUDES NO COMÉRCIO ELETRÔNICO

## Análise de Risco

- Sistema integrado de análise de risco: a inteligência aplicada na solução do problema
  - Compartilhamento de informações
    - Permite a análise de histórico de transações no comércio eletrônico como um todo – perfil típico
    - Viabiliza checar “velocity” com eficiência

# USANDO INTELIGÊNCIA NO COMBATE A FRAUDES NO COMÉRCIO ELETRÔNICO O Futuro

- Adoção de novos meios de pagamento e surgimento de novos meios de fraude
- Novos métodos de autenticação
  - 3D Secure (Verified by VISA, SecureCode)
- Certificação e assinatura digital

**USANDO INTELIGÊNCIA NO  
COMBATE A FRAUDES NO  
COMÉRCIO ELETRÔNICO**



***OBRI GADO***

*Walter Hannemann*

*walter@ciashop.com.br*

*FControl (www.fcontrol.com.br)*