Bringing the Customer into Audit

Steven Murdoch
University of Cambridge
Has chip-and-pin failed to foil fraudsters?
It was supposed to bring an end to unauthorised card transactions, but two years on is chip-and-pin just as fallible as its predecessor?

Danny Bradbury
The Guardian, Thursday 3 January 2008

This is a big week for Alain Job. The 40-year-old football coach is bringing his case against the Halifax bank to court. He says that fraudsters withdrew £2,100 from his account at ATMs, even though he was in possession of his card, and he doesn't want to pay.

Chip-and-pin was supposed to stop disputes like this. First introduced to the UK in 2004, it replaced signatures with chips embedded in bank cards that verify a customer's four-digit pin. Cards also contain a secret key used to validate the card with the bank.
Job case

Disputed ATM withdrawal

Audit logs destroyed by bank

Card destroyed by bank
We also requested at the time of this claim, supporting documents from [redacted] and were provided a copy of the till receipts confirming these charges were verified with the PIN. These receipts also show the products purchase which was for three separate charges of £3000.00, £4000.00 and £2500.00 for currency in Euro's and not for a holiday as thought by [redacted] at the time.

Timings and location of these charges are as follows.....

£3000.00 - 20/05/08 - 12.27pm
£4000.00 - 20/05/08 - 12.28pm
£2500.00 - 20/05/08 - 12.30pm

All made at [redacted]

Unfortunately CCTV was requested for the period of these charges but unfortunately the disk had been recorded over so was/is not available.
AmEx case

Disputed PoS transactions
No refund despite known vulnerability
Card destroyed by customer

We also tested the time of this claim, supporting documents from and were provided as proof of receipt confirming these charges were verified with the PIN.

These receipts show the products purchased which was for three separate charges of £3000.00, £4000.00 and £2500.00 for currency in Euros and a holiday, though by the time.

Timings and location of these charges are as follows...

£3000.00 • 20/05/10 • 12:27pm
£4000.00 • 20/05/10 • 12:30pm
£2500.00 • 20/05/10 • 12:30pm

Unfortunately CCTV was requested for the period of these charges, but unfortunately the disk had been recorded over so was not available.
A change in the way that banks deal with victims of fraud is being demanded after Santander suggested that a customer was stealing from his fiancée so that it did not have to refund £10,000 in disputed transactions.

The man won his year-long battle to clear his name only after a bank worker was arrested for fraud. Santander then refunded the £10,000, but not before requiring her to sign a confidentiality agreement binding her to secrecy.

The case raises concern that Santander is routinely suggesting that customers are criminals to deny them refunds.

Peter Vicary-Smith, the chief executive of Which?, said:

"Santander’s behaviour in this case was absolutely shocking. The last thing you need when you discover someone has cleared out your account is for your bank to say it was your fault.

"To claim that chip-and-PIN is infallible is simply not a strong enough argument for accusing a customer of negligence or fraud."
Disputed ATM withdrawal

Card destroyed by customer

Woolf case

Refund after arrest for fraud
Internal audit is not working

- Incentives
- Poor procedures
- Buggy software
- Regulatory capture
- Insufficient auditing
- Poor interpretation
- Lack of communication
Bank records:

Below is a list of the dates and times of all transactions performed in [redacted] from 23rd July 2009 onwards. I have also included further computerised records for your information:

<table>
<thead>
<tr>
<th>Date</th>
<th>Amount</th>
<th>Retailer/ATM</th>
<th>Successful/Unsuccessful</th>
</tr>
</thead>
<tbody>
<tr>
<td>24/07</td>
<td>211.66</td>
<td>Unsuccessful</td>
<td></td>
</tr>
<tr>
<td>24/07</td>
<td>3994.56</td>
<td>Successful</td>
<td></td>
</tr>
<tr>
<td>24/07</td>
<td>3994.56</td>
<td>Successful</td>
<td></td>
</tr>
<tr>
<td>24/07</td>
<td>3187.54</td>
<td>Successful</td>
<td></td>
</tr>
<tr>
<td>24/07</td>
<td>85.56</td>
<td>Unsuccessful</td>
<td></td>
</tr>
</tbody>
</table>

According to our records, all successful transactions were authorised with the genuine card and correct Personal Identification Number (PIN). Therefore, whoever performed these transactions had access to your card and had full knowledge of your PIN. A cloned card was not in operation.
Merchant record:
oxo8 = PIN entry required, PIN pad present, but PIN not entered
Help the customer help you!

AmEx case

Woolf case

Job case

Disputed PoS transactions
discovered by
bank

Card destroyed by customer

Disputed ATM withdrawal

Card destroyed by bank

Audit logs destroyed by
bank

*From case Woolf case

No refund despite known vulnerability

Refund after arrest for fraud

Help the customer help you!

Internal audit not work

Buggy software

Incentives

Regulate

Insufficient auditing

Lack of

Internal audit not work
Help the customer help you!
Do not destroy the card

- Card maintains a transaction counter (ATC)
- Card (optionally) maintains a transaction log

Use these to catch fraud
Cryptographically protect logs

- Maintain hash chain over customer account events
- Print on statement
- Publish top-level of hash tree somewhere else

Prevent log tampering
Make receipts useful for audit

- Have input to cryptographic MAC on receipt
- Force bank to give enough verification data

Verify security properties
Questions?

Do not destroy the card
- Card maintains a transaction counter (ATC)
- Card (optionally) maintains a transaction log
  
  Use these to catch fraud

Cryptographically protect logs
- Maintain hash chain over customer account events
- Print on statement
- Publish top-level of hash tree somewhere else
- Prevent log tampering

Make receipts useful for audit
- Have input to cryptographic MAC on receipt
- Force bank to give enough verification data
- Verify security properties

Help the customer help you!

Bank records:

<table>
<thead>
<tr>
<th>Date</th>
<th>Amount</th>
<th>Retailer/ATM</th>
<th>Successful/Unsuccessful</th>
</tr>
</thead>
<tbody>
<tr>
<td>24/07</td>
<td>211.66</td>
<td></td>
<td>Successful</td>
</tr>
<tr>
<td>24/07</td>
<td>399.45</td>
<td></td>
<td>Unsuccessful</td>
</tr>
<tr>
<td>24/07</td>
<td>3187.54</td>
<td></td>
<td>Successful</td>
</tr>
<tr>
<td>24/07</td>
<td>85.56</td>
<td></td>
<td>Unsuccessful</td>
</tr>
</tbody>
</table>

According to our records, successful transactions were authorised with the genuine card and correct Personal Identification Number (PIN). Therefore, whoever performed these transactions had access to your card and had full knowledge of your PIN. A cloned card was not in operation.

Cryptographically protect logs
- Maintain hash chain over customer account events
- Print on statement
- Publish top-level of hash tree somewhere else
- Prevent log tampering

Internal audit is not working
- Poor procedures
- Bugs
- Poor interpretation
- Incentives
- Poor design
- Internal audit is not working
- Lack of communication
- Regulatory capture

Incentives Poor procedures
- Buggy software
- Regulatory capture

Bank records:

<table>
<thead>
<tr>
<th>Date</th>
<th>Amount</th>
<th>Retailer/ATM</th>
<th>Successful/Unsuccessful</th>
</tr>
</thead>
<tbody>
<tr>
<td>24/07</td>
<td>211.66</td>
<td></td>
<td>Successful</td>
</tr>
<tr>
<td>24/07</td>
<td>399.45</td>
<td></td>
<td>Unsuccessful</td>
</tr>
<tr>
<td>24/07</td>
<td>3187.54</td>
<td></td>
<td>Successful</td>
</tr>
<tr>
<td>24/07</td>
<td>85.56</td>
<td></td>
<td>Unsuccessful</td>
</tr>
</tbody>
</table>

According to our records, successful transactions were authorised with the genuine card and correct Personal Identification Number (PIN). Therefore, whoever performed these transactions had access to your card and had full knowledge of your PIN. A cloned card was not in operation.