

Frequent card-use fraud profiling

Insurance application underwriting and processing

Debit & Credit Card repeat use tracking

Paper and voice notes conversion

Cheque tracking and use profiling

Money laundering modus analysis

Mortgage application underwriting and fraud detection



### Fraud Search & Prevention

**Credit card fraud** with complex use behavior  
**Debit card fraud** with cross-institution mapping  
**Cheque fraud** with feature, use and location tracking  
**Mortgage fraud** with document analysis with other known fraudulent applications  
**Internal fraud** with technique indication  
**Corporate loans and asset fraud**  
**Insurance claim fraud with indicator tracking**  
**Funds movement** mapping  
**Account moves** with repeat modus  
**Identity theft** with trend analysis  
**Incident and case file**  
**Fraud records and repetition**  
**External search with law enforcement** and immigration records where available  
**External search** for news and related indicators on Internet related information sites

### The ATM/ABM System

**Tracking card use**  
KS products monitor activity at the ATM and debit card processing stations, automatically analyze card information, exact time stamp, exact location and merchant etc. the system maps use against the use-database and compares results against a rule system to determine whether or not to notify security analysts for card suspension action.

**Cheques, Mortgages, insurance and loans**  
Ks products operate for all document and instrument type by using scanners, voice conversion for mapping use against previous use and other known documents.

### Storage and archive

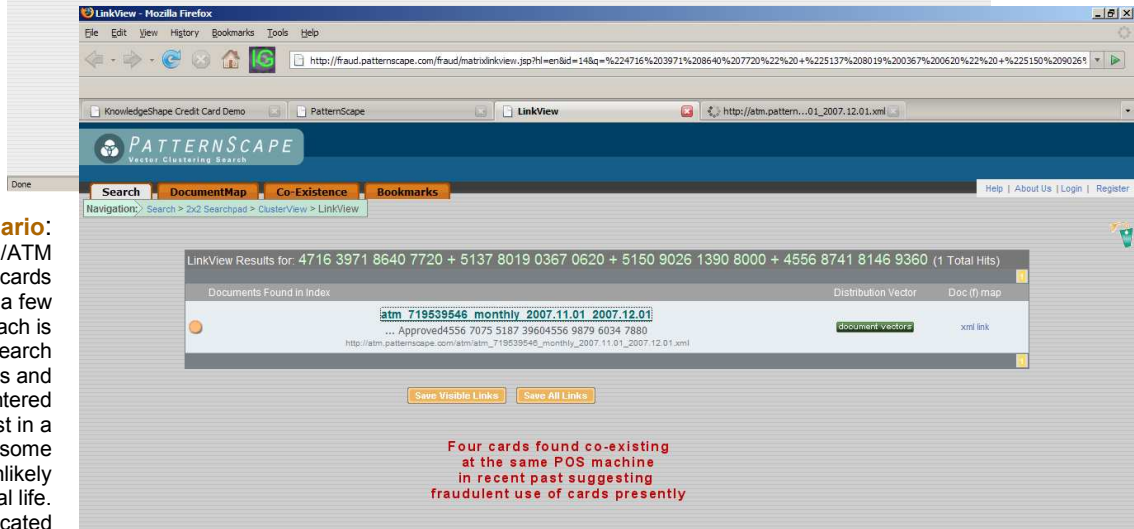
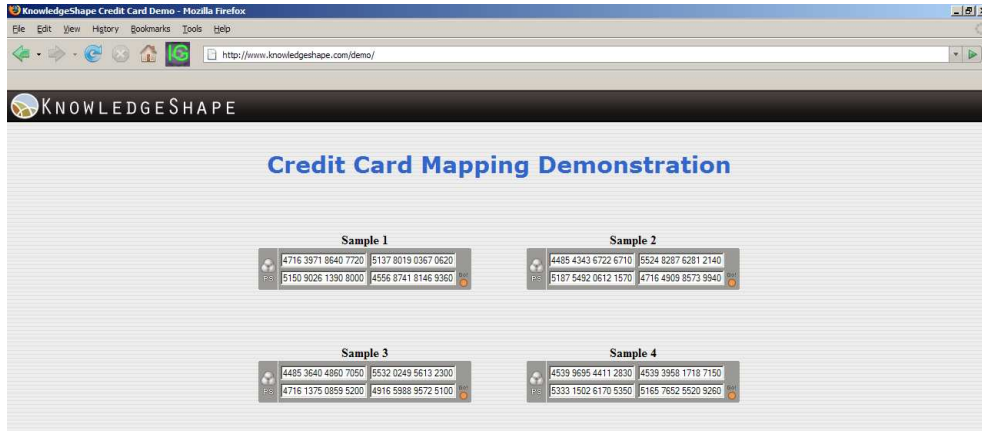
**Instant document retrieval** with high speed search regardless of document type, location and volume

**Voice dictations** conversion, storage and search

**Paper records transcription automation**  
Information transformed into searchable editable assets for speedy transcription

**Long-term storage** and conversion of paper based instruments, computer based files and voice recordings

**Instant search and retrieval** of archived documents based on content.



Four cards found co-existing at the same POS machine in recent past suggesting fraudulent use of cards presently

ICICI ATM: 719539546

From 2007/11/01 0:0:0 GMT To 2007/12/01 0:0:0 GMT

Location: 4479 Jade St Richmond BC CA V7E 2E4

Transactions	Card No	Withdrawal Amount	Expiry Date	Transaction Timestamp	Transaction Status
	4539 4131 5659 6490	40.0	10/2010	2007-11-1 0:11:30	Approved
	5114 9241 8197 5710	160.0	05/2009	2007-11-1 0:16:42	Approved
	5212 8865 8326 9530	40.0	10/2009	2007-11-1 0:29:51	Approved
	4916 2027 2822 7160	160.0	01/2009	2007-11-1 1:00:23	Approved
	5393 9190 8724 1040	120.0	03/2008	2007-11-1 1:04:52	Approved
	4532 3622 6417 6970	100.0	03/2007	2007-11-1 1:06:42	Approved
	5314 8993 4857 8330	80.0	02/2009	2007-11-1 1:09:27	Approved
	5161 6428 3789 8720	140.0	09/2008	2007-11-1 1:19:02	Approved
	4929 7315 6792 0870	80.0	01/2007	2007-11-1 1:46:31	Approved
	5578 7583 9606 7730	2000.0	09/2011	2007-11-1 2:27:33	Approved
	4916 9039 0013 1190	100.0	10/2008	2007-11-1 2:35:55	Approved
	5222 8369 0311 3620	40.0	04/2009	2007-11-1 3:01:16	Approved
	4716 7591 0838 4870	100.0	02/2009	2007-11-1 3:04:46	Approved

**The Fraud Scenario:** Four different ABM/ATM machines receive cards from users over a few minutes. Each is submitted for search clustering analysis and four cards being entered are found to co-exist in a POS machine at some past date-an unlikely event for normal life. Thus fraud is indicated and the cards are submitted to the hot list and an alert is emailed to security analysts for kill or suspend action. In the event of a mass attack these four cards provide the system with enough information to create the POS hot list for Killing or Suspending all cards within the date these four co-exist. Result: financial loss prevention.

Figure 1: The automatic debit card entry system

Figure 2: The resulting ATM/ABM machine that four cards co-exist as a past event

Figure 3: The ATM/ABM device where the cards were likely skimmed. In this case a day event list