

Card Fraud Mitigation for Credit Unions: An Overview of Card Processor Fraud Tools



CSCU

Building relationships. Strengthening credit unions.



JAVELIN STRATEGY & RESEARCH

SYNDICATED RESEARCH
CUSTOM RESEARCH
STRATEGIC CONSULTING

April 2011

Introduction

Credit unions, like all financial institutions, need to be vigilant in combating fraud. With card-not-present (CNP) fraud and counterfeit cards on the rise, credit unions are affected by the very same fraud threats afflicting larger issuers. In 2010, fraud on existing card accounts presented a massive loss of \$14B to the industry, with 4.5M consumer victims of credit and debit card fraud.¹

In today's market, there are several card processors providing a suite of fraud prevention and detection solutions. These range from your standard neural network to neural network-enhancing services and data compromise management solutions, as well as more consultative fraud analyst support services. Unlike larger financial institutions with access to budgets and resources to invest in a wide variety of fraud solutions, credit unions must be more selective and economical in the types of solutions they choose.

In an effort to provide an educational guide to credit unions of all sizes, this report provides an overview of the various fraud tools offered by some of the leading card processors operating in the credit union space. Among those included are FIS, TSYS, JHA Payment Processing, First Data and Fiserv. Data from a November 2010 survey of CSCU member credit unions is also featured, showing members' usage of fraud solutions and perceptions of where card fraud is headed in the coming year.








¹ 2011 Identity Fraud Survey Report, Javelin Strategy & Research, February 2011.

Overview of Card Processors

This section provides an overview of several well-known card processors operating in the credit union space. The table below breaks down each processor's experience and background in serving the credit union industry. A summary of each processor's fraud management solutions is also provided below and on the following pages.

Card Processor Industry Tenure/Market Share


	Card Processor				
					
Credit Union Industry Tenure	More than 30 years	More than 25 years	More than 30 years	Recently entered the CU processing market	More than 30 years
Current Share of the Credit Union Market	Supports two of the largest CUSOs in the country and most state CU leagues	Roughly 2,500 credit unions as of September 2010	Smaller share of the market	Smaller share of the market	Over 1,200 CUs
Credit Union Client Base	Mix of CUs, all sizes	Large/midsize CUs	Mostly smaller CUs	1-2 large CUs, remaining are smaller CUs	Mix of CUs, all sizes
Notable Credit Union Clients	Suncoast Schools FCU, Alaska USA FCU	**	Redstone FCU	Navy Federal Credit Union	**
CUSO Partnerships	CSCU, CO-OP	**	**	BancVue	PSCU, TMG, Indiana Credit Union League, and TNB (A Fifth Third company)

** Information not provided

© Javelin Strategy & Research

Overview of Card Processors

Card Processor Fraud Tools

Fraud Products Overview	Card Processor				
					
Core Solution (e.g. neural network)	Fraud Alert Management (Falcon)	eNFACT (Falcon)	Live Monitoring, plus PRISM Neutral Network (Retail Decisions)	TSYS Card™ Guard (in-house developed solution)	Real-Time Authorization Decisioning (Falcon)
Complementary Solution to Core	FIS Secured™	eNFACT Real-Time, eNFACT Case Management	**	TSYS CardGuard Real-Time Decisioning	DefenseEdge Real-time Decisioning
Chargeback Management Services	Yes	Yes	***	***	***
Data Compromise Management Services	Compromise Manager™	Card Tracker	***	***	***
Fraud Analyst Consulting Services	Applied Analytics™	Risk Office	***	***	***
Loss Guarantee	Yes	***	***	***	***
Fraud Education	Webinars, whitepapers, training	Webinars, whitepapers	Webinars, whitepapers	Webinars, whitepapers	Webinars, whitepapers, training
Support	24-7, 365 days	24-7, 365 days	24-7, 365 days	24-7, 365 days	24-7, 365 days

*** Product not available

© Javelin Strategy & Research

Overview of Card Processors



What FIS offers:

- FIS offers a comprehensive suite of fraud products and services. FIS solutions integrate layered rule and score-based fraud strategy deployment along with Visa® Advanced Authorization risk data elements and MasterCard® strategies.
- FIS offers 24/7/365 fraud monitoring; transaction scoring and case management; cardholder contact, account status updates and issuer notification; and real-time authorization decisioning at the point-of-sale. Full-Service and Self-Administered service options available, providing CU flexibility.
- Enterprise level solutions that can detect and prevent fraud across all FIS platforms, including platforms recently acquired through the eFunds and Metavante acquisitions.

Differentiating points:

- FIS has a comprehensive suite of complementary fraud tools designed to address all aspects of card fraud.
- Only FIS offers a warranty against fraud losses resulting from lost, stolen, or counterfeit debit and credit cards.
- FIS employs an in-house team of fraud analysts, decision scientists and PhD-level statisticians that focus on optimizing fraud strategies.
- Custom CU fraud strategy deployment and fraud analytic consulting available through FIS' Applied Analytics™ program.
- FIS offers a multi-platform fraud process, providing clients with credit and debit fraud strategies.



What Fiserv offers:

- Fiserv provides a variety of fraud management solutions, with enFACT being its primary fraud prevention/detection solution.
- enFACT is a Falcon-based system for fraud detection that comprises a neural network, daily reports, cardholder notification, direct contact with cardholders, and a call center of analysts combined with an automated voice response unit to assess the likelihood of fraud.

Differentiating points:

- Fiserv is highly effective in reducing fraud losses. On average, Fiserv's clients have reported roughly 3-3.5 basis points in fraud losses; the national average in 2009 was 7.5 basis points.
- Fiserv offers Risk Office, an investigative and consultative service designed to manage the business impact of fraud. This aims to detect the cause of fraud incidents and determine solutions and strategies for mitigating exposure.

Overview of Card Processors



What JHA offers:

- JHA provides an array of fraud management services, with Live Monitoring and PRISM Neural Network representing its core solution.
- JHA offers standard fraud detection capabilities, including name and expiration date mismatch detection, address verification service (AVS), BIN/account spending limits, card activation, PIN and verification code validation.

Differentiating points:

- Flexibility in implementing adjustments to fraud rules. JHA aims to work closely with credit unions to deploy new rules that lower false positives.
- Customization with regards to changing rules and updating the neural network based on the most recent fraud trends.



What TSYS offers:

- CardGuard is TSYS' cornerstone fraud solution, comprising an in-house neural network that evaluates for risk and pinpoints potential fraud patterns. CardGuard is integrated with clients' processing systems and incoming authentication information.
- TSYS also maintains a partnership with Falcon, leveraging Falcon scores along with its own proprietary internal scoring.

Differentiating points:

- TSYS has the ability to proactively reach its client base in advance of Visa CAMS alerts.
- TSYS has a full integration of tools, FICO scoring and CardGuard rules.
- There is open discussion among fraud managers. Clients can call in to talk about rules they've built and trends they're seeing. TSYS maintains a group of clients that network together.

Overview of Card Processors



What First Data offers:

- First Data's core fraud detection solution is its FICO scoring platform, which can be further enhanced by its own proprietary decisioning system, DefenseEdge.
- Credit union clients can access all tools/reports via StarStation, a web portal that allows for clients to manage existing rules and implement new rules. Clients can share information on transactions they would like to charge back, and First Data works with the appropriate association to resolve them.

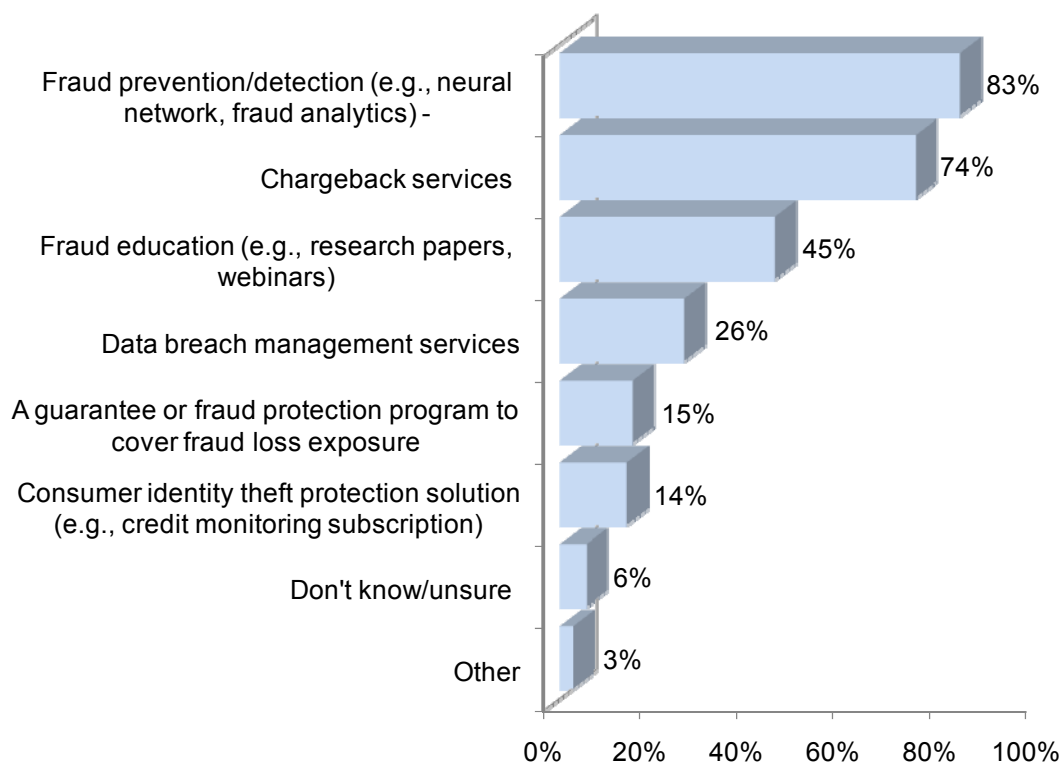
Differentiating points:

- Customer insight data is a newer service offering that allows clients to see fraud trend information at a glance and engage in peer-to-peer benchmarking, all in real-time.
- First Data offers flexibility with rules. Clients can opt to have rules drafted/maintained on their behalf, supplement rules with their own policies, or draft and manage their own rules.

CSCU Member Survey Results

What Fraud Tools are Credit Unions Using?

More than 8 in 10 CSCU Members Using Fraud Prevention Tools



Data collected from an online survey of CSCU members reveals that 83% of those surveyed are utilizing a basic fraud prevention/detection for mitigating credit card fraud, while 74% report they are taking advantage of the chargeback services. Nevertheless, less than half of members are utilizing the fraud education provided. In addition to CSCU's webinars and online fraud education resources, members can tap into instructional design type courses and FIS' Fraud Portal. Members can stay apprised of latest fraud trends via CSCU's quarterly fraud newsletter, in addition to regular email/web updates.

CSCU Member Survey Results

Examples of CSCU member feedback on FIS fraud tools are provided below:

“A greater tendency to pick up fraud trends and when something does seem strange for our credit union, they will reach out to us and make recommendations for Flash Fraud rules.”

“I think that [FIS] has a wonderful program for fraud. Their fraud department is very knowledgeable and they are very helpful in trying to help our members understand why they are calling them regarding fraud on their accounts.”

“FIS is always on top of the charges for our card members. If there is unusual activity, we will get a report to let our card members know. We have stopped fraud in many cases quite quickly.”

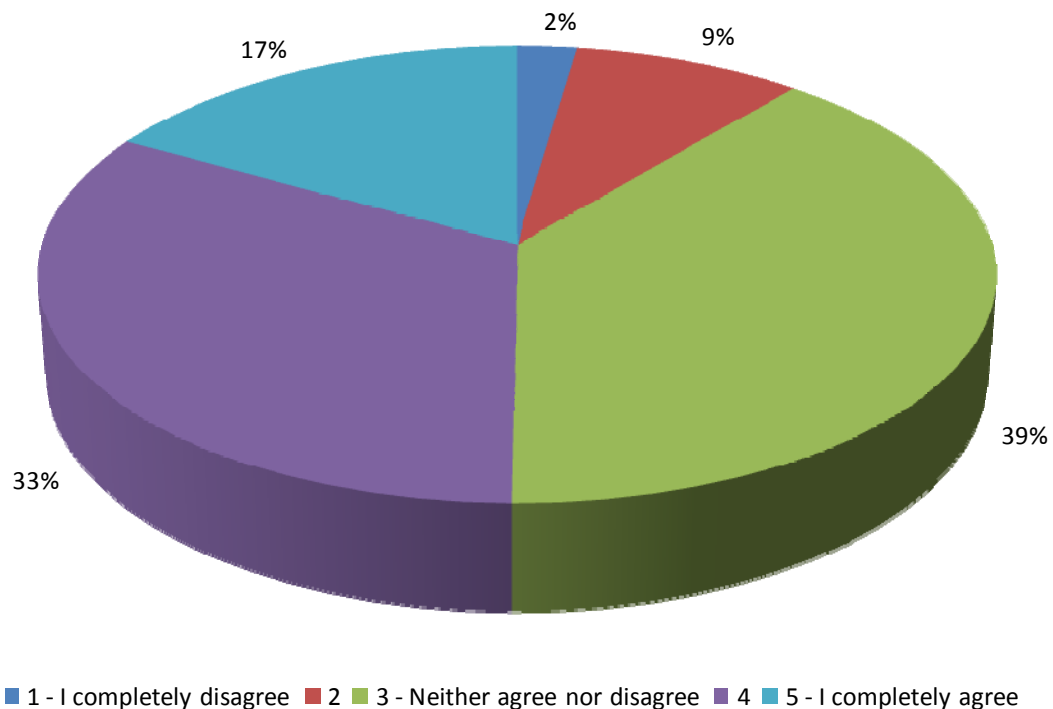
“Our fraud is detected early, which minimizes losses, and their chargeback services are exceptional in that we recover most of the fraud loss in a lot of situations.”

They are always accessible. They are quick to notify both the credit union and the member for fraud or potential fraud issues. They send information via e-mails to keep us up-to-date on educational and informational resources.”

CSCU Member Survey Results

One in Two CSCU Members Believe in Additional Investment in Fraud Technology

“I believe my credit union should invest in the latest or more up-to-date fraud solutions offered by our card processor”



Despite strong satisfaction ratings for current fraud tools, members noted the need for more up-to-date fraud prevention/detection offerings. Data revealed one in two survey respondents believe their credit union should invest in the latest fraud solutions offered by their credit card processors. Several of the card processors interviewed for this research paper indicated plans for rolling out new fraud prevention solutions in 2011, either designed to enhance core solutions or address fraud threats not previously covered. Credit unions are encouraged to regularly check in with their card processor to learn about new offerings and potential solutions that may strengthen their fraud management program.

Case Studies

American Credit Union

American Credit Union (ACU) is a credit union with just under 5,000 members. Javelin Strategy & Research interviewed ACU's Office Manager to obtain a smaller credit union's perspective on a situation in which their card processor stepped in to successfully handle a fraud situation.

ACU's response to the Heartland data breach:

"...the fact that we had all these faxes coming over in a matter of hours, it was 'What the heck is going on? We are being attacked', and right away we were re-pulling our authorization reports and looking for weird activity. I guess that we came in on Saturday to contact our cardholders, and as we were trying to figure out what was going on with that breach, we were in close contact with FIS. We actually devised a matrix and we were literally writing down date, time, merchant, location, trying to figure out what do these transactions have in common and I did send all that information over to them. As we were finding certain things like cash transactions, they were altering Falcon as they were getting information, and they were able to re-program Falcon in hopes to catch additional fraud. I think that was fantastic, and I think the people that we worked with during that time were very open to receiving the information that we had and the ideas that we had, and they kept us in a loop with things that they were discovering. They also developed that other website where we can go in and share information with other credit unions and get additional information such as alerts or test vendors, things of that nature. So I think they have been very proactive when it comes to fraud."

Eastman Credit Union

Eastman Credit Union is the largest credit union in Tennessee with over 108,000 members. Javelin Strategy & Research interviewed Eastman's Card Manager to provide an example of a situation in which their card processor stepped in to successfully handle a fraud issue.

Eastman's response to Falcon alerts:

"We have quite a bit of card activity. The last month I looked at was August, and we had about 1.4 million transactions going through our card systems. Falcon, I would say, catches probably 20 cases a month, perhaps even 25 -- and that is significant to us. [The fraudulent transactions] are large amounts and they do stop these, which is very helpful."

Case Studies

Eastman's response to the Heartland data breach:

"I will say, as much as we had a fraud and the losses we experienced, they would have been easily doubled. But because Falcon did have that in place, they were stopping them. They were quick to identify the fraud, and once the trend began and Heartland really started rolling, they had already tightened up their parameters."

Recommendations

- 1. Comprehensively understand what your card processor's fraud tools really have to offer. In considering your fraud solution's performance, think about the following:**
 - What are your processor's fraud scoring capabilities (real-time, one-time, batch)? Are the rules neural, linear, or behavioral? Any financial institution should have the option for both real-time and batch scoring.
 - Is your fraud detection system being exposed to the right data at the right time? This is critical in effectively managing false positives.
 - How easy is it to handle the fraud situation once the transaction has been confirmed as fraud? This depends on how tightly your credit union's fraud management systems are integrated with the other processes that must be invoked.

- 2. Ensure your institution is maximizing the full value of the fraud solutions offered by your card processor.**
 - Invest heavily in fraud analytics; rules are only as good as the analytics driving them.
 - Fraud analytics need to continually evolve in response to ever-changing fraud threats and will ultimately impact the success of a credit union's overall risk strategy.
 - Thorough review of processor-provided data reporting, such as Excessive Authorization Reports and Foreign Activity Listings, for example, is a key component of an effective strategy.

- 3. Quantify your institution's fraud mitigation progress.**
 - An institution that manages fraud well should be able to quantify it. A credit union that can measure its results in terms of fraud-loss ratios is a shining example of an institution that is keeping a keen eye on its ROI.
 - Establish internal trending benchmarks to better track fraud performance:
 - Gross vs. net fraud loss
 - Fraud loss percentage of transaction volume
 - Average loss per fraud case and transaction
 - Percentage of fraud loss by type (e.g. Counterfeit, CNP, Lost/Stolen, etc.)

- 4. Have a formal risk management strategy in place.**
 - Implement a formal risk management program that allows your institution to make informed decisions about your fraud strategy.
 - Review your strategy periodically to ensure optimal performance and compare to industry-recommended best practices:

Recommendations

- Authorization parameter thresholds (e.g. daily card spend limits, velocity controls, etc.)
 - Decline mismatched CVV/CVC, expiration dates, and names
 - Formalized procedures for verification of address changes, as well as new PIN or plastic requests
 - Frequently inspect ATM façade, card reader, and PIN pad for tampering
- 5. Take advantage of the educational resources offered by your card processor.**
- These resources may come in the form of webinars, research papers, in-person fraud round table discussion, newsletters, web site updates, training, and other activities.
 - Regularly participating in these events and reading up on updates will keep your institution informed not only on the latest fraud trends but also on any new developments pertaining to your fraud solution.
 - Member education to help prevent being victimized by phishing, identity theft, etc.

Methodology

Data for this research paper was collected on behalf of CSCU by Javelin Strategy & Research. In-depth phone interviews were conducted with risk/fraud product managers of each of the card processors featured in this study. Secondary online research was also gathered on the card processors and their fraud solutions. In-depth phone interviews were conducted with credit unions for the case studies.

261 CSCU members were surveyed online in order to obtain quantitative data on product usage and general opinions regarding fraud mitigation.