



# Is Your Risk Monitoring System Risky?

## *New spin on old fraud compromises debit accounts and makes portfolios vulnerable*

By Laurie LeBoeuf

One of the older schemes in merchant fraud is issuing credits/refunds with no offsetting sales. Over the years, the scheme has changed as the industry catches up and updates the monitoring systems.

In the earliest version of the fraud in question, perpetrators would just issue refunds with no offsetting sales to credit cards. The industry learned to look for negative batches. The fraudsters then began issuing credits with no offsetting sales and would then run a charge for the exact same dollar amount on a stolen credit card. This would make the batch zero or slightly positive. The industry caught up by making the risk monitoring systems look at all credits and reconcile them to offsetting sales on the same card numbers.

Along the way, the fraudsters learned that if you run the returns on check cards, they would have access to almost instant cash instead of having to wait around for the issuers to send checks out. All of the earlier frauds were performed using the credit card networks.

In the latest fraud scheme, the perpetrators are issuing credits with no offsets, but risk monitoring systems are not picking up on the transactions.

Traditional monitoring systems are set up to review the transactions flowing through the credit card networks. Many acquirers do not monitor PIN-based debit networks. In the past, the debit networks have involved little risk because:

- PIN-based transactions validate who the cardholder is, so there are very few chargebacks.
- Issuers typically limit PIN-based debit transactions to \$500 or less per day.
- Some acquirers do not hold any liability for chargebacks through the debit networks.
- Credits cannot be run through the debit networks.

But the latter is no longer true. Typically, the ability to issue credits/refunds through the debit side of the terminal is



disabled. However, the fraud perpetrators have discovered how to turn this feature on in the terminals and sometimes at the network level. If the transactions from the debit networks are not flowing through your risk monitoring system or are not being reviewed, you're at risk.

Refund fraud is especially appealing to the perpetrators because the money is available very quickly. Oftentimes, once the fraud has been committed, the acquirer has difficulty stopping it. Most of the processors lack an easy way to prevent this fraud. FDR, for example, has a feature called Real Time Fraud, which will allow the acquirer to delete the batch as long

as it is caught prior to settlement. First National Merchant Solutions can delete a batch as late as the following day after settlement and is probably the most effective system currently.

Most processors' only option is to perform credit reversals. Even for the ones who have systems in place to delete batches or transactions, if the fraud is detected too late, the credit reversal is the only way to potentially undo some of the damage. Some processors charge huge fees to perform the reversal, and they aren't guaranteed to work. Credit reversals are tedious, time sensitive, and don't have to be honored by the issuers.

# the X factor!

when it comes to **mobile payment solutions**...eXperience counts!

with more eXperience developing advanced "future proof" payment solutions EXaDigm gives you...

- ▶ a highly secure, truly modular, PC-based mobile payment terminal
- ▶ offering more features than any other terminal available today
- ▶ with unparalleled eXcellence in service and support
- ▶ for the same price (if not better) than the others

## so what?

**retain** merchants longer | **increase** residuals faster | **grow** your portfolio value sooner!

what the others can only promise, EXaDigm delivers!



XD2100SP

▶ Mobile Payment Terminal



RX Series

DX Series

UX Series

▶ Wireless Modem Options



▶ Cellular Wireless Plans



the X factor...eXperience delivering true innovation in **Mobile Payment Solutions**. To learn more contact ExaDigm at **1.866. EXA TEAM** or visit us online at **www.exadigm.com**.

goes  
where  
others  
can't.



### The MTT 1510 fits the Mobile Merchant

WAY Systems developed the smallest POS in the industry to provide mobile merchants with a first class service that will grow their business. The MTT 1510 gives merchants “**transactions without boundaries,**” with the power to accept payment anywhere at any time.

Available through [www.unitedbankcard.com](http://www.unitedbankcard.com)  
United Bank Card  800.201.0461



WAY Systems, Inc. is the exclusive worldwide licensee for pocket-sized merchant POS solutions based on granted patents held by Fractal Commerce, Inc. (WO 99/66752). The patents cover communication method and apparatus improvements for all GSM, GPRS and 3G-enabled POS devices used for authenticating payment transactions.

Here are some steps you can take to protect yourself:

1. Find out if, on the back end, you can disable the feature that allows refunds through the debit network. If it is available, then turn it off.
2. If the controls are only available at the terminal level, incorporate a password system to limit access to downloads. As you know, more terminals than not have default passwords that are never changed.
3. Find out if your monitoring system is looking at both the credit and debit networks. If it is not looking at debit networks, fix it. It is only a matter of time before the fraudsters figure out yet another way around them once the door is open.
4. Find out now how your processor handles reversing credits so you have the steps in place for damage control, if it becomes necessary. Ensure your staff know where to access this information; inevitably, fraud will occur on a Saturday or on a skeleton crew.
5. Keep your risk people actively involved with the International Association for Financial Crimes Investigators IAFICI. If a fraud occurs in your business, your risk managers will need connections to issuers and the IAFICI is a great bridge ([www.iafci.org](http://www.iafci.org)).
6. Keep your risk people actively involved with the Merchant Acquirers Committee so that they can keep up with current changes in fraud.
7. If you are hit with a new type of fraud, pass the word on. A loss is a loss to the industry and benefits no one. There is no competition in risk; changes in fraud trends should be openly shared with everyone. You do not have to disclose information about the perpetrators, but it is important to let everyone know if you are seeing something new.

Fraud is ever changing. Ensure your risk-monitoring system is robust enough to make changes as needed. Don't be the one the crooks know can't make updates quickly. Fraud perpetrators will find your vulnerability and then share that information with others. You don't want your company on the list of easy targets. **TT**

---

*Laurie LeBoeuf is vice president of operations for Rapid Advance in Bethesda, MD. Reach her at [laurie@rapidadvance.com](mailto:laurie@rapidadvance.com).*

# In Today's World of Uncertainty and Change Service, Reliability and Performance are Key



As your trusted partner for end-to-end payment processing and related support services, TSYS Acquiring Solutions delivers robust point-of-sale processing with the highest level of service and a dedicated commitment to security, reliability and compliance—all to help you grow your merchant portfolio with confidence.

**TSYS Acquiring Solutions offers:**

- >> Single Authorization Platform
- >> Rapid Merchant Boarding
- >> Superior Uptime Metrics
- >> World-Class Service and Support
- >> Reporting On Demand
- >> Compliance Expertise and Leadership

To learn more about how we can help you achieve growth that outperforms the industry, give us a call at **480.333.7799** or email [sales@tsysacquiring.com](mailto:sales@tsysacquiring.com) for a speedy response.

**Every Second. Every Hour. Every Day.**  
Impeccable Performance Delivered.

**TSYS** Acquiring Solutions

[www.tsysacquiring.com](http://www.tsysacquiring.com)