



LASCO POSITIONING STATEMENT

Lasco provides Information Technology (IT) solutions for small to mid-size financial institutions, businesses and organizations across the Upper Midwest. Lasco also serves as a data processing center for financial institutions providing numerous bank services to assist institutions with their day-to-day operations. For almost 40 years, Lasco has worked in an honest, ethical manner with its commitment being to assist its clients in achieving success. Lasco's client relationships are built on this commitment and trust with each of its clients.

Note from the CEO:

Dear Valued Customer:

As I am sure you are aware, Michigan's economy is one of the weakest in the country. According to recent reports, Michigan is ranked the 50th state on personal income growth, unemployment rates and employment growth. These statistics are affecting the businesses in the Upper Peninsula as well.

I would like to express my gratitude and appreciation for your relationship with Lasco. By partnering with Lasco we are jointly supporting the Upper Peninsula's economy by keeping the monies in the U.P. By continuing to work together we can hopefully help the U.P. tread water until the economy of the State starts to turn positively.

Warmest Regards
 Dennis VanLandschoot
 President/CEO

Lasco Signs with UP State Bank, Range Bank

2007, marking Lasco's 40th year in business, was also significant in welcoming two additional banks to Lasco's Check 21 Solution and Merchant Capture Solution. UP State Bank of Escanaba partnered with Lasco on January 26th for remote image branch solution and Range Bank followed on February 10th. The additional banks expand Lasco's ability to operate with clients amid multiple host interfaces and continue to advance Lasco's status as the leading Check 21 processor of the Upper Peninsula.

Direct Merchant

As distributed capture solutions continue to build momentum across the U.S., the driving force of paper to electronic gives rise to an increasing range of Check 21 solutions. Lasco is expanding services to include direct merchant capture, which brings distributed capture directly to corporate and merchant clients.

With direct capture, check images are captured as close to point of receipt as possible. Merchants scan their own checks, convert to check images and electronically transfer them to the bank.

Lasco offers the Smart Deposit solution, designed using Microsoft Smart Client capabilities. Smart Deposit operates behind the point of presentment and allows a fully functional capture application without requiring immediate connectivity. Features of the system include IQA (Image Quality Assurance), electronic coding through CAR (Courtesy Amount Recognition) and LAR (Legal Amount Recognition), user-definable fields and transmission. The system will also automatically detect duplicate checks and recognize if the deposit is out of balance.

Direct capture solutions are increasingly implemented because merchants can easily track and manage their deposits by transmitting them directly to the bank and receiving same-day credit.

This reduces or eliminates the need for couriers, encoding, capture and handling checks. Lasco's Direct Merchant is designed to bring convenience and cost-effectiveness to the user in order to maximize cash flow.

For further information on Lasco's DirectMerchant solutions, please contact Dennis VanLandschoot, President/CEO, at 800-800-6197, extension 151 or direct at 906-228-1057.

VoIP

Traditional phone calls work by allocating an entire phone line to each call. With VoIP, voice data is compressed and transmitted over a computer network. This means VoIP uses substantially less bandwidth than a traditional telephone call and is consequently more cost effective. Here are some other benefits:

- **Simplified infrastructure.** With VoIP on your network you no longer need separate cables for your telephone system.
- **Scaleable.** Traditional PABX (Private Automatic Branch Exchange) based phone systems come in many size ranges and it may be necessary periodically to scrap existing systems and replace hardware; this is not the case with VoIP systems.
- **Reduce operating costs.** Because a VoIP exchange is based on software rather than hardware, it is easier to alter and maintain.
- **Improve productivity.** VoIP treats voice as if it were any other kind of data, so users can attach documents to voice messages or participate in virtual meetings using shared data and videoconferencing.
- **Flexibility.** A Virtual Private Network (VPN) is an allocated amount of bandwidth on the public Internet where public access is prevented through encryption. If your company has its own VPN and combines it with VoIP, you can set up a fully functioning office anywhere with a broadband connection.

Initially, it makes sense to introduce VoIP as an addition to your existing PABX-based system and gradually increase your level of sophistication as and when you need more functionality. An important strength of VoIP architecture is that it can operate side-by-side with your existing systems. By initially restricting the roll-out of VoIP to a single department such as sales, and then extending it to the rest of the business as your needs dictate, you can minimize disruption and stagger your costs.

If you decide to use VoIP, it is essential to check out the robustness of the networks you will be relying upon to ensure smooth implementation. Voice communication is far too important for it not to work reliably in all conditions.

You need to look at these main issues:	Quality of service	Technical support
	Reliability	Security

Lasco has the ability to bring you VoIP solutions to your business and assist you with realizing these cost savings. If you would like more information on how Lasco can assist you, please contact Dan Fezatt, Senior Vice President – Operations at 800-800-6197, extension 157 or direct at 906-228-1057.

Prepaid Debit Cards

As a means of reinforcing your current customer relationships and expanding relationships beyond those current customers, prepaid debit cards present a wealth of opportunities. Your own prepaid debit program can generate revenue from interchange, activation, usage and maintenance fees.

Gift cards issued by retailers are the most familiar form of prepaid debit, but financial institutions may utilize prepaid debit in a variety of ways. A study by Dove Consulting found that 65 percent of consumers reported buying or receiving a gift card within the past year. Although retailer-issued cards dominate the market, ten percent of purchasers said they had given cards issued by financial institutions.

While developing a prepaid program, it is essential to realize beforehand what market segment is being targeted, and what your objectives are. Afterwards, you will want to consider if you want cards that are part of a closed-loop (specific vendors) or open-loop network (not specific vendors). Also, consider if the cards would be most appropriate as disposable or reloadable. With disposable cards, consumers spend a pre-defined value and dispose of the card after use, whereas reloadable cards allow the consumer to put additional amounts on the card. Another consideration is what kind of transactions you want the cards to support (such as ATM access and bill pay). It is also important to recognize state regulations that affect prepaid card sales.

Travel cards present a convenient alternative to traveler's checks, and offer limited reload capabilities. A **family card** is a reloadable card for general use, with an expiration date. Parents may monitor the use of the card online and can control funding of the card for their children. Family cards have the advantage of establishing an early relationship with the younger people using the cards, who will be in the position to choose your bank later on. **Incentive cards** give your corporate customers a way to reward their employees, which will also promote your brand to these employees. **Payroll cards** will do the same.

Metavante offers a wide range of prepaid debit options. For more information, go to the Products and Services page at metavante.com. Click on Prepaid Debit Card Account Processing under EFT Solutions.

Original article found in NYCE's [Payment Strategies](#), Volume 1, Issue 2.

Special Security Section

Protecting Private Information

It is thanks to the Internet that so many activities have become easier. The unfortunate flip-side to that coin is that accessing your personal information is no exception. That personal information may be addresses, phone numbers and birthdates, or the more sensitive information of Social Security numbers, credit card and bank account numbers.

Privacy advocates and professional investigators do say that some steps can be taken to protect and/or remove some of that information; however it may not be possible to erase all traces of your information online.

Basic search engines can turn up information in things like newspaper articles, blogs and online forums. Websites (ZabaSearch, for example) are available in which people can search for personal information that turns up not only addresses and phone numbers, but criminal and sex-offender records, bankruptcies and relatives. Even property records, voter lists and court filings can be found online. With the proliferation of blogs and social networking like MySpace, more and more detailed information about you can be available on the Internet.

The most effective way of protecting personal information online is to avoid giving it out. Avoid signing up for supermarket loyalty cards and sweepstakes and avoid mailing in warranty cards. While in chat rooms, blogs, online forums, etc. be mindful of the information you are providing. You can try not to include your email address when filling out forms on websites in order

to limit spamming. Of special importance, before giving out your Social Security number to anyone, it is a good idea to find out why it is needed, how it will be used, and how it will be protected.

Many sites that include personal information in search results do provide the option of allowing you to request your name to be removed. Sites that want to validate identity may require mailing or faxing a copy of a driver's license or some other form of government identification (as Intellius Inc requires), and may ask for other details like email and mailing address and Social Security number.

The solution may be short-term because many sites do not remove you from actual records or databases, meaning that when the online lists are updated, your information may appear again. When the sites are monitored frequently, however, it can be an effective method of removing much of your personal information online.

There are also some services that offer to assist in removing personal information from directory sites. For a monthly charge, MyPublicInfo Inc. offers an Identity Sweep, which will fill out the required opt-out forms for you from various sites and monitor them to ensure the information does not reappear.

Legislation is being advocated to require states to remove or block certain sensitive details online, and to develop a consumer-notification law for security breaches of personal information, which could potentially include exposure of personal information to unauthorized parties on the Web.

Creating a Safe Password

How safe is your password?

Passwords are usually cracked through “dictionary” attacks, where software tries out combinations of common phrases and words. The words are often checked in combination with various “appendages” that include two and three digit combinations, symbols and dates. They may also use substitutions such as “3” for “E.”

The cryptographer, computer security specialist and author Bruce Schneier recommends using a root word and putting an appendage in an unusual place in the word – which could be somewhere in the middle or at both the beginning and end. He suggests using a word that is not in the dictionary – for example, a word you can pronounce, but which is misspelled, such as “baysball.” Attaching the appendage to this word (bay1776sball, or 4920baysball9483) would create a password that is not easily cracked by this kind of software.

Cyberattacks

Websites that allow users to contribute content make it easier for hackers to do the same. When content comes from outside sources, as in the case of personalized Web pages that allow messages to be posted from other users, and that allow utilization of basic software code to change the appearance of the page, the content cannot always be considered safe and trustworthy. Hackers can use links and computer code on these Web pages to spread viruses and steal personal information.

MySpace, Google, eBay and Wikipedia.com have all been targeted by these kinds of cyber attacks in the past year. On Wikipedia.com, the online encyclopedia that can be edited by anyone, a hacker created a fake entry about a supposed virus in Microsoft Corp. software, and included a link that users could follow to supposedly download a protection from the virus. Instead, the link led to a site that, itself, downloaded a virus. In the case of Wikipedia, its founder Jimmy Wales says that Wikipedia users likely will take care of the problem themselves by removing bad links, as in the case of the supposed Microsoft virus hacker, whose link was removed within a minute of it being posted. (The hacker then simply routed users to links that led to an older version of the article, and all of the versions of the article finally had to be removed by an administrator in Germany.)

MySpace does plan to confront these security issues, and is working on more standardized procedures to deal with security issues; eBay also uses “scrubber” technology to comb sites for pieces of malicious code that can be found when users incorporate programming codes into their auction listing pages.

As the risk of cyber attacks on user-generated content Web pages continues to spread, some firms have also partnered with certain online companies featuring user-generated content to help them address these security issues. Some expect security solutions to be provided by Web companies in the future, in the same way that email users who were previously expected to buy their own spam-filters provided to them through email services of Internet service providers.

Original articles for the security section found in The Wall Street Journal in January 29, 2007 Technology section and Yahoo news at <http://tech.yahoo.com/blogs/null/13353/how-to-pick-a-genuinely-secure-password>.