



CU SOLUTIONS



Partnerships Powering Pennsylvania Credit Unions

Facing Today's Unprecedented Risks & Threats

Today's credit unions are facing unprecedented risks and threats to their operating environment—everything from criminal and fraudulent activities to natural and man-made disasters—making it critical for credit unions to stay ahead of emerging risk trends. Just about any product, service or process may expose your credit union, including employment practices and internal controls to physical threats, such as robbery and natural disasters, to ACH fraud, data breaches and identity theft. Let's not forget about the increased regulatory requirements in place to ensure your credit union is safe and sound with its business practices.

“Risk can never be entirely eliminated, but using risk assessments as part of an enterprise-wide risk management strategy will help credit unions continue to provide meaningful products and services to members while including necessary safeguards to protect the credit union.”

—Ann Davidson, Senior Risk Management Consultant, CUNA Mutual Group

IDENTIFY, MEASURE, CONTROL

By implementing a formal risk assessment process that identifies, measures and controls inherent risks, you can address the vast array of complex and ever-changing risks and industry regulations troubling credit unions today.



Your risk assessments should answer these questions: What can go wrong? How can it go wrong? What is the potential impact? What preventative measures can be taken? How can it be stopped from happening again or at all?

RALLYING EXECUTIVE SUPPORT FOR RISK AND COMPLIANCE INITIATIVES

The challenge is to translate the benefits offered by risk management into something more relevant. Avoid using the rhetoric of security advantages and focus on

continued on next page



Take an Enterprise Approach to Security

Today's security professionals must play dual roles—proactive assessors of threats and stewards of the credit union's resources. They thwart old-school robberies and burglaries, while responding to evolving threats, such as electronic fraud and organized crime. In addition to protecting assets, they must now monitor, manage, and maximize resources.

These realities present a unique opportunity to broaden the view of credit union security. Instead of the traditional single-branch approach, security professionals can look across departments, sites and channels.

A SINGULAR VIEW OF MULTIPLE TOUCH POINTS

Diverse consumer touch points are the hallmark of a successful credit union. From multiple branches to off-premises ATMs, mobile banking to the online channel, credit unions are available wherever their members are, ensuring meaningful, convenient banking experiences.

Historically, each location—each touch point—within a credit union has been viewed as a discreet security implementation. Each site had its own unique security approach and, oftentimes, its own security partner for services, such as alarm monitoring. However, there are disadvantages to such a disparate security operation. This inefficiency is accelerating the movement toward an enterprise approach that encompasses administrative offices, data and customer service centers,

branches, off-premises deployments, retail delivery channels, data and networks.

MAKING SECURITY A POWERFUL BUSINESS TOOL

Considering how security can add value to other organizational operations is another way to break from the traditional security approach. This broader view can make security a meaningful, powerful business tool.

A value-driven approach leverages security resources to deliver value to other parts of the organization. For example, cameras can be used to monitor consumer traffic/flow, assess the result of training initiatives, measure the effectiveness of marketing campaigns and more. This approach enables security to drive return on investment (ROI) throughout the enterprise, leveraging security technology to help credit unions achieve specific business objectives.

RELYING ON A TRUSTED PARTNER

Partnering with a trusted security provider can make today's dual security role more manageable. Security success can be accelerated when credit unions forge relationships with a single-source advisor that takes an enterprise approach to security. An effective partner can engineer solutions that leverage networks and migrate traditional security systems into an integrated services platform. That partner can utilize emerging solutions and enable credit unions to streamline security and

continued from previous page

the financial argument—properly implemented security technologies will save a credit union money.

Forester Research reports that the average security breach can cost between \$90 and \$305 per lost record. In other words, failure to protect data can be many times more expensive than deploying an appropriate solution. Another burden is lost employee productivity. If employees are diverted from their normal duties or contractors are hired to respond to data breaches, your credit union can incur unexpected, and often substantial, additional expenses [[Read more](#)].

CHANGE APPROACH TO MANAGING FRAUD

Fraud is not going away, and criminals are working harder and becoming more sophisticated in their quest to steal from businesses, financial institutions and individuals. To thwart their activities, credit unions need to rethink their approach to managing fraud risk and no longer silo-monitor fraud within each product area of your credit union.

It's not a matter of *if* fraud will occur, but *when*. Getting to the root cause of fraud is critical—know what controls are already in place and where there may be gaps to fill [[Read more](#)]. 🛡️

sources: [CUNA Mutual Group](#), [TraceSecurity](#)

focus on core responsibilities. And that partner can deliver managed or hosted security services that can meet objectives for business process improvement. You need a managed security services partner that understands today's threats, a partner like [Diebold](#).

Contact your Association [Account Executive](#) for more information. 🛡️

Tackle Security Risks With a One-Two Punch

Many credit unions feel they cannot be proactive in their information security risk management because it is simply a luxury they cannot afford. However, nothing could be further from the truth. What they've failed to calculate is the cost of not mitigating risk. Simply put, a security breach or data loss can cost significantly more in both time and money than properly handling the risk to begin with, and that is exactly where proactive risk management comes into the picture. It all comes down to the cost of not doing business as opposed to the cost of doing business.

PROACTIVE RISK MANAGEMENT MAKES BUSINESS SENSE.

Shoring up your credit union's data security requires more than just plugging in new software and expecting it to thwart all threats. It's a complicated endeavor. It requires an expert combination of assessments and protection tools. That's why your credit union can benefit from the expertise of these powerful alliances from [CUNA Strategic Services](#): [TraceSecurity](#) to analyze your credit union's unique

vulnerabilities, and [SilverSky](#) to follow up and protect against future threats.

RISK ASSESSMENTS & COMPLIANCE SOLUTIONS

Because a credit union's information technology (IT) security systems are interdependent, it's helpful to have a trusted partner that can see the whole picture and deliver an effective, orchestrated, dependable, end-to-end assessment.

[TraceSecurity](#) provides risk management and compliance solutions to protect critical data and meet IT security mandates. With a unique combination of people, processes and technology, TraceSecurity provides a holistic view of your credit union's security posture.

Offering a full range of assessments, testing, and security training to ensure compliance and reduce IT risks, its market-leading services include:

-  Security and risk assessments;
-  IT security audits;
-  Internal and external penetration testing;

-  Web application testing;
-  Wireless assessment;
-  Social engineering analysis; and
-  Security training

NETWORK & EMAIL SECURITY

[SilverSky](#) adds that next critical layer of protection: comprehensive network and email security, to effectively guard your credit union's infrastructure.

Any attack can bring down your network, create security compliance issues and damage your credit union's bottom line—possibly, its reputation as well. To avoid a harmful breach, you must guard every part of your credit union's infrastructure—from desktop computers to servers.

SilverSky safeguards networks with comprehensive intrusion prevention, firewalls, anti-spam, anti-malware and Web filtering. Solutions include:

Managed security services: using event monitoring and response, unified threat management and network device management;

Network protection suite: including vulnerability management, Web security, mobile device management, log management and brand protection; and

Email protection suite: including advanced DLP, email archiving, email continuity and AV/AS and encryption.

Regardless of your credit union's size and IT skill set, security threats (both internal and external) exist, and having an active, comprehensive program in place is your best defense.

Simply put, the combined solutions of TraceSecurity and SilverSky can be the perfect 1-2 punch to meet growing network security needs. Contact your Association [Account Executive](#) today! 

Check out these great resources:

[TraceSecurity Blog](#) and
[SilverSky Knowledge Center](#)



Preventing Account Takeovers & ACH Fraud

Today's fraud landscape is becoming more complex, featuring extensive intertwined risks—some old, but with new wrinkles and some emerging at the pace of new technologies. These emerging risks require credit unions to adopt rigorous, cross-channel fraud monitoring strategies.

Regardless of how the fraudsters get in, their end game is financial gain and how they accomplish that continues to evolve. Realize that a particular fraudulent act may not directly or immediately result in a loss but may later manifest itself in another form. Fraud prevention measures are vital, but knowing where fraud is occurring and plugging the hole is even more important.

ONLINE BANKING & ACH FRAUD LOSS—THE ANSWER IS IN ADVANCED TRANSACTION MONITORING

In an effort to keep in step with member expectations, credit unions across the country now offer online banking. This creates an unprecedented level of convenience—members can complete all their banking needs without ever having to walk into a branch or meet a teller face-to-face.

Unfortunately, with the increased convenience comes a downside: online banking fraud. Sophisticated fraudsters are exploiting the growing reliance on Internet banking to steal and launder money. The problem has reached such proportions that in June 2011, the Federal Financial Institutions Examinations Council (FFIEC) issued a supplement to their 2005 guidance entitled [Authentication in an Internet Banking Environment](#). The supplement is a response to an increasingly hostile online environment and makes clear that since the release of the original guidance, the threat landscape has shifted dramatically.



While it seems nobody is safe from cyber criminals, it is corporate accounts, particularly those of small and mid-sized businesses (SMBs) that are facing some of the heaviest focus from cyber criminals. A June 2012 Symantec Intelligence Report revealed that 36 percent of all targeted attacks since the start of that year were directed at businesses with 250 or fewer employees.

How exactly are they doing it? One common method is account takeover. This involves the undetected installation of malicious software (malware) on a computer that accesses the member's online bank account. Commonly, in the case of a corporate account takeover, the criminal will manipulate payment information (e.g., adding new payees to

the payroll or altering account numbers of payees). The money is then transferred via the ACH channel to the accounts of individuals who will then move the money to a place where the cyber criminals can safely access it.

HOW DO WE PREVENT THE STAGGERING LOSSES THAT OFTEN RESULT FROM ONLINE ACCOUNT TAKEOVERS?

The answer is in a layered approach to security, with behavior-based transaction monitoring at its core. This is a defense-in-depth approach, providing multiple layers of frustration for the criminal, with the greatest protection at its center. Behavior-based

continued on next page



Check & Card Fraud: Stopping it at the Door

Everywhere you turn, there is an industry alert popping up and we expect our tellers to know each and every one of them. The fraud department may know about them, but even they need help keeping up and organizing the alerts.

Imagine if your tellers had access to 90 percent of the accounts in the United States right at their fingertips.

Over the years, [Advanced Fraud Solutions](#) (AFS) has been compiling a national counterfeit database from the industry alerts, as well as through an organized grass roots approach: Community Counterfeit Watch. Access to this national database is available through the AFS **TrueChecks™** solution which analyzes demand drafts for frontline personnel, giving real-time decisioning power on check acceptance and recommendations on appropriate Reg CC hold. In a nutshell, the TrueChecks solutions stops counterfeit checks at the

teller workstation without compromising the integrity of service.

And through a collaborative effort with Early Warning Services, AFS developed the web-based **DEPOSIT CHEK™** solution which can be available at every PC within your credit union. The DEPOSIT CHEK service is at the forefront of helping protect financial services organizations by providing advance notification of high-risk deposits.

DEPOSIT CHEK is a proven solution to help prevent fraud and expedite funds availability decisions at the teller window, new account desk, image ATM, online banking and/or the back office.

DEBIT AND CREDIT FRAUD PREVENTION

The challenge in card fraud is knowing where the source of the crime took place. Was it the local diner, the online purchase or maybe the WIFI connection

continued from previous page

transaction monitoring helps credit unions analyze account holder activity in the context of the person's (or business account) normal behavior and highlights anomalies.

It is the early detection of anomalous transactions and the speed of response that offer the surest form of protection against fraud in the ACH channel. Transaction monitoring technology that allows a credit union to detect anomalies before ACH files are transferred to the Federal Reserve for payment can have an enormous impact on preventing fraud loss, protecting members' accounts and, in turn, preserving a high level of trust in the existing relationship between member and credit union.

To learn more about ACH fraud and the most effective ways of preventing it, download a free [Remote Banking Fraud Detection for Dummies](#) e-book from Verafin. CUNA's endorsed partner for BSA/AML compliance and fraud detection, [Verafin, Inc.](#), is a provider of advanced, behavior-based fraud detection and anti-money laundering (FRAML™) software utilized by financial institutions across North America. ♥

at our favorite eatery? Regardless, card investigators are challenged daily with pinpointing the point of compromise. That's where **TrueCards™** comes into play. TrueCards enables you to independently identify plastic card compromises and skimming cases and determine precisely which cards are at risk almost immediately. You simply block the cards at risk and save untold thousands of dollars.

To learn more about **DEPOSIT CHEK**, **TrueChecks**, and **TrueCards**, contact your Association [Account Executive](#). ♥

Counterfeits represent 30% of the check losses.

Return deposit items represent an additional 30% of the check losses.

Foil Fraud With New Account Decisioning

According to the 2011 ABA Deposit Account Fraud Survey Report, attempted check fraud against banks' deposit accounts amounted to an estimated \$11 billion in 2010 and check fraud losses estimated \$893 million. In today's highly-competitive and highly-regulated landscape, new account departments need to focus on two things: 1) More accurately identifying good members, and 2) Stopping fraudsters at the door.

An effective new account decisioning tool should quickly and efficiently differentiate between potentially good members and high-risk applicants—while generating as few false positives

as possible. Not only does this improve member service, it also protects the bottom line.

“In the new regulatory environment, credit unions are increasingly focused on the profitable growth of their member base ... [And] the data integrity of decisioning solutions has a critical role in facilitating this growth. Credit unions are looking for solutions with high levels of data integrity and transparency to help minimize false positives and enable intelligent risk-based decisions.”

—Julie McNelley, Senior Analyst, Aite Group.

identity verification and compliance list screening.

Enlisting Deluxe Detect typically results in 20- to 25-percent cost savings for most financial institutions. Additionally, Deluxe Detect clients share that efficiency at the new accounts desk has increased dramatically—up to 30 percent in some cases, largely because of the customizable responses. (Source: Deluxe Survey)

The robust features of Deluxe Detect can help you stop more fraud, open more accounts, improve the member experience, increase profitability and enhance operational efficiency. Best of all, you won't need to make any platform changes or pay higher fees. Download the [Deluxe Detect Information Sheet](#). 

Here's another great resource:
[Deluxe Knowledge Blog](#)



4309 North Front Street
Harrisburg, PA 17110-1618

www.pcu.org

**Contact Your Association
Account Executive**
cusolutions@pcua.org

Central Pennsylvania

Russell Evans
AVP, Business Development
russell.evans@pcua.org
800-932-0661 x 5330

Western Pennsylvania

Monika Edlis
Sr. Account Executive
monika.edlis@pcua.org
717-503-7348

Eastern Pennsylvania

Angelique Pattillo
Account Executive
angelique.pattillo@pcua.org
717-884-5847



When was the last time you evaluated the performance of your new account fraud screening system? Deluxe invites you to compare your current provider to [Deluxe Detect](#)[®], one of the industry's most effective tools for screening applicants. It uses configurable business logic and some of the industry's most predictive data for identity verification to help you identify applicants with a prior history of fraud and/or account abuse, while also performing

