Combating Fraud in Today's Environment

Bank of America Merrill Lynch

Bank of America Merrill Lynch continues to focus on cybercrime and understands it is the responsibility of banks and clients to help secure online banking sessions. Banks need to deliver appropriate security measures and clients should leverage all the fraud prevention tools that banks have made available. Security education for clients is a key piece of any bank's layered security offering, as security education is an industry best practice.

There is no "silver bullet" to eliminate security breaches; therefore industry best practices call for multiple layers of security tools. Fraudsters typically take the path of least resistance when attempting to breach online security. Companies who use all the security tools available and attend security education webcasts are typically less likely to be impacted by fraud. Client education is a strong mitigant against fraud.

Due to the heightened risks with Internet usage, as well as the mobile fraud landscape, increased client diligence is recommended. Clients should work with their banks to help protect against fraud. The eCommerce security strategy is twofold: a layered security model, using best-in-class security tools, along with strong client security education.

Layered security

Our award-winning treasury management platform, CashPro® Online, features a layered security model.

CashPro Online provides the following security tools to help clients protect against online fraud:

- PC device registration
- Two-factor authentication at login
- Mandatory dual administrative approval for high-risk user entitlements
  - Single approval with a token may be available to clients who, due to the size of the company, are limited to one administrator to establish and maintain entitlements
- Segregation of duties for user entitlement and transaction approvals
- Dollar limits for users and/or transactions
- Strong password requirements with mandatory 90-day expiration
- Validation of user credentials through an email validation code, every six months
- Non-concurrent logins
- Fraud monitoring, with alerts and a dedicated fraud monitoring team
- Transaction behavior logging
- Email notifications for designated online activity are sent to administrators for review
- Audit Logging of critical events with the ability to expand or narrow the scope of your review according to your business parameters and analytical needs
  - Client controls should include a regular review of audit logs for suspicious activity.

Client education

As an advocate for proactive security education, the eCommerce security team conducts fraud landscape webinars and publishes white papers on best practices to approach security education. For clients who cannot attend scheduled webinars, the sessions are recorded and available with security white papers and user guides. These resources are available in CashPro Online through CashPro® University.