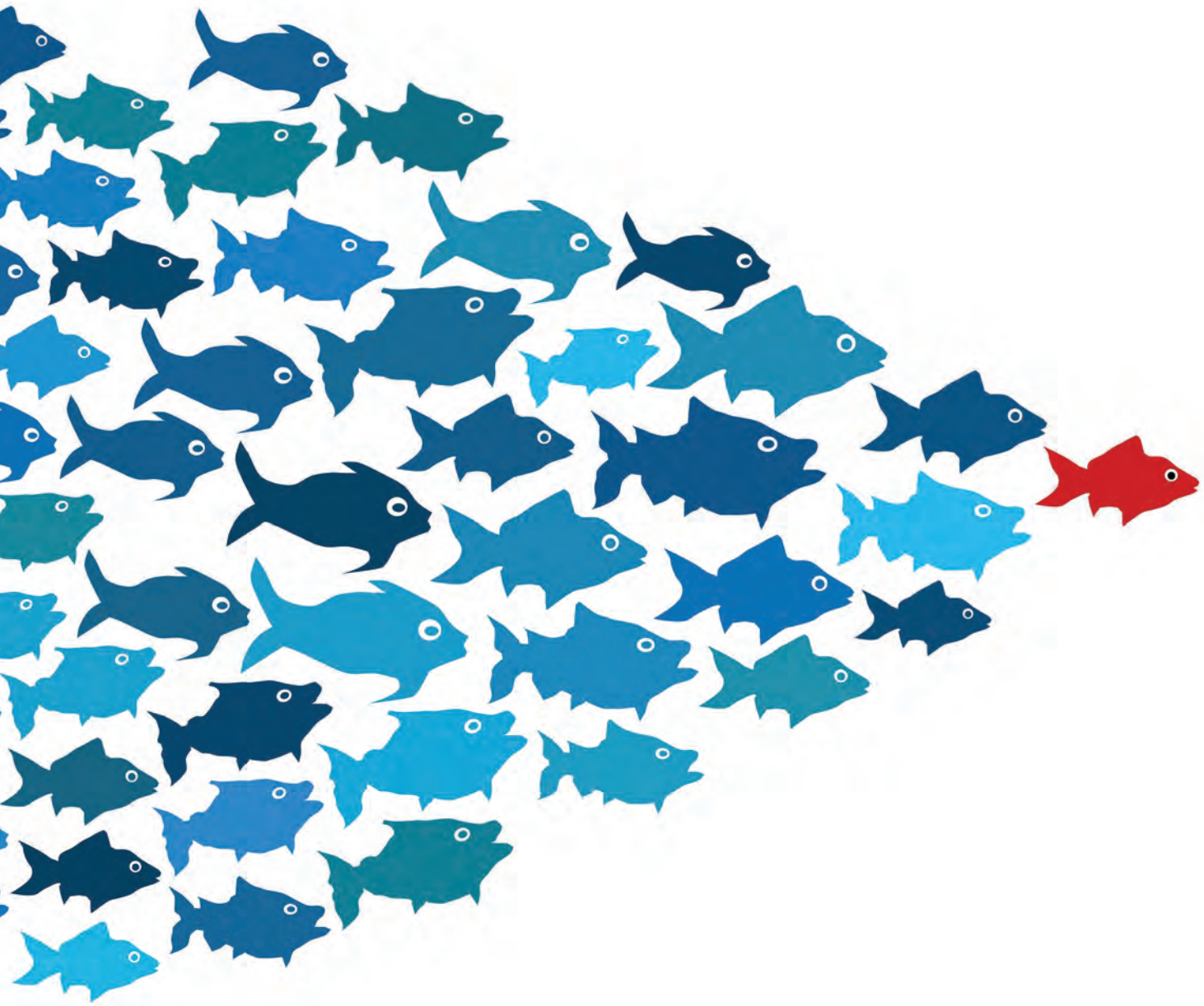
STAY ONE STEP AHEAD



SPONSORED SPECIAL REPORT

E-retailers can leverage technology and tactics to avoid falling prey to cyber criminals

CYBER CRIMINALS AREN'T RESTING. They're constantly finding new ways to defeat retailers' data security and fraud prevention systems—whether they're stealing millions of credit card accounts in one fell swoop, perpetrating fraudulent transactions or finding new vulnerabilities to exploit.

That means retailers that let their guard down risk becoming the next high-profile victim of a data breach that shakes consumers' confidence in their brand and costs money. Staying ahead of criminals requires retailers to regularly evaluate their security and fraud prevention systems to spot weaknesses criminals can exploit.

"Fraud prevention and data security is an arms race that retailers can't afford to fall behind in," says Justin Morgan, information security officer for payments processor Litle & Co., a Vantiv company. "Criminals are becoming better at using technology to enter a retailer's system and strike unnoticed."

Bridging the gap

Retailers can stay ahead in the risk management arms race by sharing consumer behavioral data across their various sales channels. Doing so provides retailers a more complete picture of fraud patterns. This capability is especially important for retailers with robust online and offline operations, according to Jeff Sawitke, chief product officer for Verifi Inc., a provider of risk management and electronic payment solutions for card-not-present merchants.

"If the merchant launches a new channel on another platform or through a third party, access to customer data from other channels may be limited or not available for use in fraud screening," he says. "Data-sharing limitations increase a merchant's fraud risk because those orders may not get the same level of review and validation as orders in other channels. That creates a weakness in the merchant's system criminals can find and exploit."

Retailers should apply the same fraud tools used in existing channels to new channels. "If a retailer is using IP address verification on its e-commerce site, it should be using it for the mobile site too," Sawitke says. "The goal is to create a consistent, singular view into customer behavior across all sales channels. Then, as it relates to fraud management, the retailer should tune its strategies to each channel."

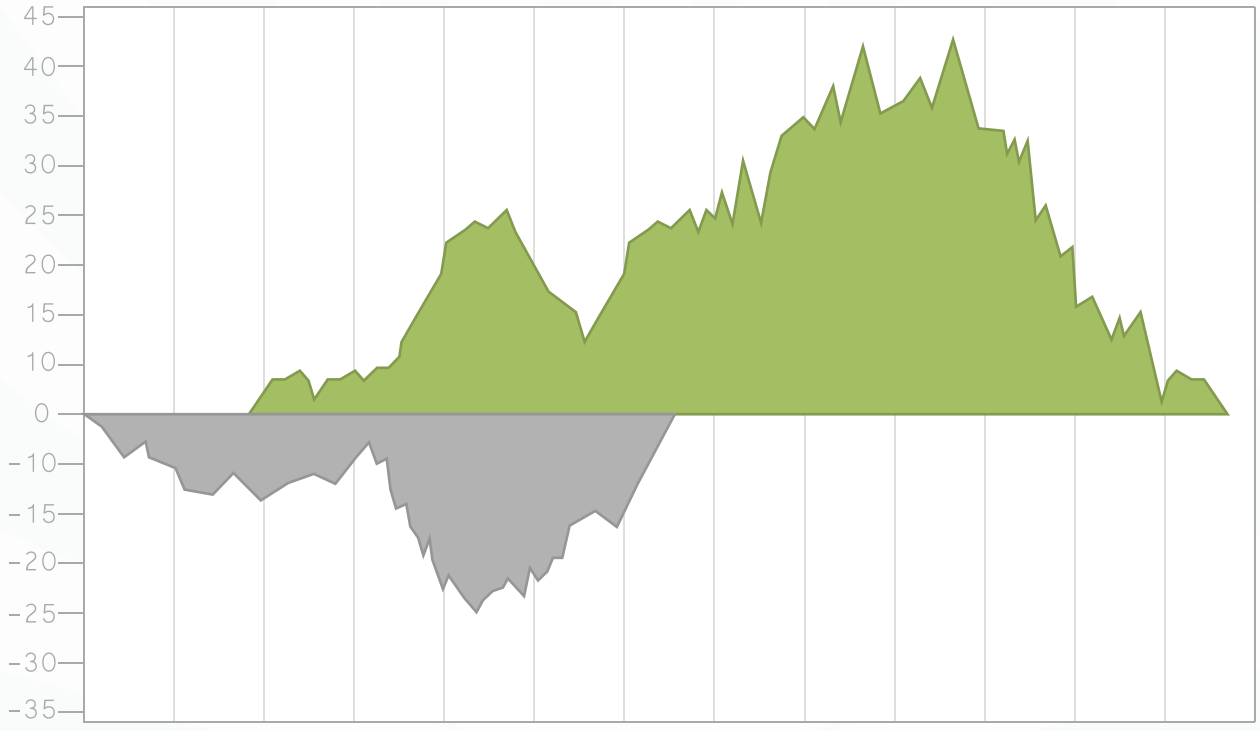
Leveraging consumer behavioral data across channels makes it possible for retailers to move away from rules-based fraud detection models that use a series of predetermined fraud screens, such as orders originating from countries with high incidence of fraud, toward more sophisticated "neural models" that score a transaction's risk based on behavioral attributes, such as sudden spikes in spending or purchase velocity. Parsing those behaviors helps improve a retailer's ability to distinguish fraudulent transactions from legitimate transactions with each transaction it reviews.

GREG WOOTEN
Chief executive officer at fraud detection services firm SecureBuy, a SignatureLink company

"Using 'big data' to identify fraud requires the right analytical engine to dig deep and uncover anomalies in the behaviors that indicate potential fraud," says Greg Wooten, chief executive officer for SecureBuy, a SignatureLink company, and provider of dynamic fraud detection applications. "From a fraud perspective, the goal is to use big data to create a safe and stable shopping environment that allows retailers to attract customers and grow their businesses."

The vendor's SecureBuy Powered with FICO tool combines neural technology, which identifies relationships between complex data sets to detect fraud patterns and learns as it goes, and adaptive analytics that score transactions by comparing current transaction behavior to recent known fraudulent and non-fraudulent behavior. This combination allows retailers to automate the fraud-screening process. The vendor integrates its cloud-based screening solution, which it developed using technology from analytics and credit scoring firm FICO, into the checkout page.

When a transaction's score exceeds the merchant's risk threshold the customer is prompted to authenticate herself



Your payments tell a story.

ARE YOU LISTENING?

There's big data behind your payments.

Unlock this data with real-world processing solutions that help you contain costs, manage risk, and generate revenue.

Litle &Co

Experience the power of

PAYMENTS INTELLIGENCE

Contact us today. 1 (888) 998-2577 or visit www.litle.com

using SecureBuy's reengineered 3-D Secure verification, which links the customer to her credit card issuer.

"By using FICO technology we are allowing card-not-present merchants to use some of the same big-data analytic technologies that 95% of the credit- and debit-issuing banks in the United States have been using to prevent fraud for more than 20 years," Wooten says.

Tokenization

Fraudulent transactions are not the only threats posed by criminals to retailers. Part of what makes retailers highly attractive targets to criminals is the amount of credit card account data running through their systems. Many cyber criminals are focused on intercepting that data as it travels through the merchant's system to its processor and back. Once the data has been hijacked it can be resold to fraud rings.

But a retailer can use tokenization to diminish the value of cardholder data to criminals. Tokenization replaces consumers' payment card data with a software token that acts as a proxy during most of the payment process. For example, when the shopper enters his card account information on the merchant's site, the system encrypts that information and sends it directly to the merchant's processor, which decrypts it and sends it to the shopper's card-issuing bank for authorization via a secure connection. The processor then returns an acceptance or denial code to the merchant along with a token, which the retailer can store for future use should a chargeback dispute arise.

JUSTIN MORGAN
Information security officer at payments processor Litle & Co., a Vantiv company

"Because the token is a substitute card number, even if a criminal intercepts it and breaks the algorithmic code that created it, he has no access to the key that maps the token back to the original card number," says Litle & Co.'s Morgan.

Litle & Co. can provide retailers real-time tokenization as well as retroactively tokenize credit and debit card numbers a merchant has on file. Tokenization also significantly scales back what a merchant must do to comply with Payment Card Industry guidelines for protecting stored credit card data, since a merchant that employs tokenization is not storing actual card data, Morgan says.

But even though tokenization is effective at protecting cardholder data, it still won't stop criminals from attempting to pass themselves off as legitimate customers. One way to stop fraud at checkout is to have a payment solutions provider that can cross-reference transactions over its entire merchant base to identify common data elements that may indicate fraud.

For example, a criminal may simultaneously make purchases from several merchants using different credit cards in an attempt to disguise his activity. If all those orders are initiated from a computer using the same IP address, however, those transactions are probably fraudulent.

"Criminals are always looking to disguise their tracks, and having a partner that can scrutinize a larger pool of transactions outside a merchant's business for fraud can significantly increase a merchant's chances of spotting fraud before an order ships," says Verifi's Sawitke.

Another way to detect potentially high-risk transactions is cross-referencing card accounts and customer data with previous transactions that resulted in chargebacks. "Chargeback data should be part of a retailer's fraud prevention tools," Sawitke says. "Spotting a credit card or customer that was involved in a chargeback dispute at checkout can prompt retailers to reassess the risk of that transaction."

Verifi's Intelligence Suite and integrated Rules Engine enables data to become actionable and automate standard order review procedures. This allows card-not-present merchants to compare hundreds of data points from new orders against fraud management rule sets which include merchant- and network-based data. Retailers can customize the system to flag transactions based on their risk threshold.

As criminals become increasingly tech-savvy, retailers have had to adjust. "Merchants can't expect to stop criminals using 21st century technology with 20th century tools," says SecureBuy's Wooten.

While retailers used to whitelist—or automatically approve—repeat customers' transactions to remove friction, that approach no longer works, Wooten says. "With data breaches at large merchants affecting tens of millions accounts, retailers can't afford to whitelist anyone, because even though the accounts affected in a data breach may have been shut down that does not mean data from those accounts hasn't been used to steal identities for the purpose of committing fraud down the road."

Other threats

Just as retailers need to think differently about how another retailer's data breach may increase their own fraud risks, they also need to think differently about the threat from consumers using mobile devices, which are particularly vulnerable to fraud.

For instance, merchants that have developed shopping applications with one-click checkout have inadvertently created a weak spot criminals can exploit with malware. Typically, retailers offering this convenience have stored the mobile user's account data. Criminals can obtain that data

NOW YOU CAN MANAGE PAYMENTS WITH *CONFIDENCE*

Verifi manages online payments 24/7/365, **reducing risk and raising revenues and profits.** So you can get back to your business and put your mind at ease.

OUR TOTAL PAYMENT MANAGEMENT SOLUTIONS HELP YOU

Reduce risks and improve your bottom line.
Award-winning *Cardholder Dispute Resolution Network* helps to ***PREVENT CHARGEBACKS*** **before they happen.**

RECOVER REVENUES **lost to chargebacks.**
Our *Chargeback Recovery Specialists* have a **success rate *OVER 50%.***

Increase billings, retain customers, and increase *LIFETIME VALUE* with *Decline Salvage* service.

Process credit cards *SAFELY* and *EFFICIENTLY* with *Global Payment Gateway.*

Mine your data to discover what drives fraud and ***COMBAT IT*** with *Intelligence Suite.*

PCI Certified
Class 1 Service Provider

VERIFI.COM

CALL VERIFI NOW AT (323) 655-5789
for your FREE Fraud and Chargeback Assessment

VERIFI

by surreptitiously downloading malware to the user's mobile device through e-mail or other web sites the mobile user may have visited that can access that card data.

One solution to this problem is to require mobile users to sign in to the retailer's app before it launches. "Anti-malware applications for mobile devices are not as evolved as they are for desktop computers, so mobile users don't always know if their device has been compromised," says Litle & Co.'s Morgan. "Requiring a user to authenticate prior to each purchase adds another layer of security."

Another area merchants can overlook is chargeback fraud, sometimes called "friendly fraud," which occurs when an online shopper makes a purchase then calls her credit card-issuing bank to dispute the purchase after receiving the product or service. The dispute often arises from buyer's remorse. Nevertheless, credit card issuers place the onus on the retailer to verify the transaction was legitimate. If the merchant cannot do so the charge is reversed by way of a chargeback in the consumer's favor. Verifi's Cardholder Dispute Resolution Network (CDRN) provides a solution to this problem by enabling merchants to receive fraud and friendly fraud dispute notifications directly from the issuer. Issuers and merchants can then collaborate to resolve customer disputes before they result in a chargeback.

Since disputing a chargeback can be expensive, some retailers conclude it is cheaper to accept the chargeback rather than fight it.

But retailers can turn to their payment solutions providers to gather the documentation to prove the transaction was legitimate. Verifi, for example, can work on behalf of the merchant to fight these chargebacks. The process evaluates the chargeback information and provides documentation of any anti-fraud prevention steps taken by the merchant such as IP address verification and device fingerprinting, which uses data to identify individual PCs, phones or tablets to verify a shopper's identity. This kind of additional information can strengthen the retailer's case that the consumer did in fact make the purchase, and help the retailer to reclaim significant profits lost to friendly fraud and the chargeback process.

"If the disputed charge is a recurring transaction, we can notify the merchant not to process future charges until the chargeback is resolved," Sawitke says. "Chargeback prevention and resolution are big parts of risk management."

Constant updates

With data breaches becoming a bigger concern for retailers, the need for more extensive ongoing security checks to identify vulnerabilities is imperative. "It's not enough to simply put data security tools in place and leave them," says Litle & Co.'s Morgan. "They must constantly be tested and upgraded."

The same applies for any kind of software an online retailer uses. A retailer must keep up with software manufacturers' upgrades to make sure it is not vulnerable to attack. Morgan recommends that retailers sign up to automatically receive upgrade notices from manufacturers for every application they use, including back-office applications such as e-mail. In addition, retailers should monitor their platform for abnormal events that can indicate a malware intrusion, such as changes to file logs or unauthorized data transfers out of their systems.

"Criminals are transferring smaller amounts of data over longer periods of time to avoid detection," Morgan says. "The hit–and-run tactics of yesterday are lessening; stealth is now the name of the game."

Given the ongoing evolution of fraud and data security threats, retailers can never rest on their laurels when it comes to safeguarding their web sites. Indeed, the threat of online fraud in the United States will only worsen in the next few years as Visa and MasterCard issuers roll out mandated chip cards, predicts SafeBuy's Wooten. Those chip cards use a standard called EMV, which has become shorthand for the move to the more secure credit and debit card technology.

JEFF SAWITKE
Chief product officer at risk management provider Verifi Inc.

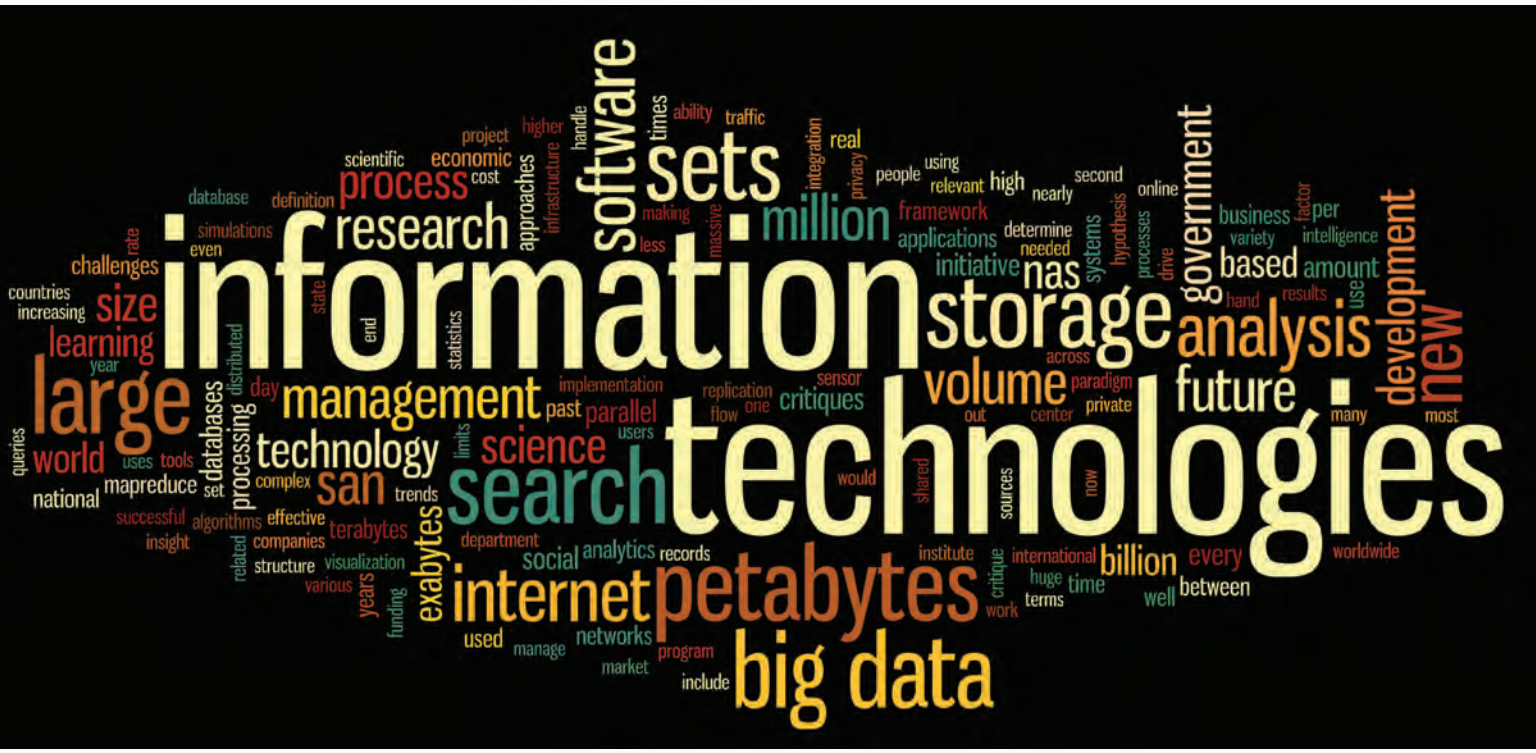
"EMV is intended to protect card data in a card-present environment, which is going to push more criminals into the card-not-present space," he says. "In every country where EMV was rolled out previously, card-not-present fraud exploded."

EMV cards prevent fraud at the physical point of sale by using a computer chip embedded in the card to validate the card to the card reader and vice versa. The cardholder authenticates himself by entering a PIN. Since online shoppers can only enter their card account and CVV number to make a purchase, the chip and PIN security features are moot.

With the October 2015 deadline for EMV rollout not far off, e-retailers must begin preparing for the expected spike in online fraud. That begins with developing a comprehensive plan for fraud prevention and data security, and communicating it clearly across all departments.

"Fraud prevention and data security has to start at the top because consumers today are demanding it," Wooten says. "It's become more of a priority for them than fast checkout. Every transaction a merchant sees needs to be assessed for risk using a multi-layered approach." ■

SecureBuy's got your BIG DATA!



100 million stolen credit & debit cards and user profiles** are flooding the payment ecosystem. Every transaction has risk...**even those consumers with a clean purchase history!

Introducing SecureBuy Powered with FICO™ -- proven card analytic technology used by 95% of U.S. card issuers and 65% of global issuers to fight payment fraud. Combining adaptive analytics, global intelligent profiling, and consortium data modeling, with SecureBuy 2.0's powerful physical attribute authentication, there is no more effective solution to take on card-not-present fraud, real-time.

- Frictionless analytic authentication for every transaction
- Adaptive card analytics - self-calibrating with every single transaction
- Reliable transaction scoring with real-time powerful physical attribute analysis
- Cloud-based SaaS scales for peak selling seasons
- Auto deployment of 3-D Secure / payer authentication for high-risk transactions
- Mobile & CNP biometric signature capture provides "compelling evidence"
- Recognizable security builds consumer trust and reduces cart abandonment
- Integrated within the shopping cart checkout process

SecureBuy®
Powered with FICO™

800-511-2050 • www.SecurebuyCommerce.com