Bank of America
Merchant Services

# Fraud is evolving. So should your data security.

## Help safeguard your company and customer data at the point of sale


The fintech industry has made huge strides in data security, including wide implementation of EMV technology and end-to-end data encryption. Yet these technologies alone aren't enough.

Chip card technology has reduced point-of-sale fraud—but bad actors are shifting their attention to card-not-present interactions such as online purchases. In fact, incidents of card-not-present fraud jumped 40 percent in the United States in 2016.[1] According to Javelin Strategy & Research, card-not-present fraud alone could cost retailers $71 billion globally over the next five years.[2]

Evolutions in fraud demand a new generation of security solutions.

"Fraud isn't going away—it's getting more sophisticated," says Larry Brennan, senior vice president of data security and director of cybersecurity at Bank of America Merchant Services. "But the security industry is always applying new techniques to keep pace."

Here's what you need to know about the current state of data security.

### FEAR FACTOR: SKIMMING, SHIMMING AND SMISHING

Fraud aimed at stealing information from consumers and businesses is increasing, both online and on the ground.

Today's data thieves are using increasingly sophisticated phishing schemes to download personal information from computers, as well as "smishing" schemes that target mobile devices. Additionally, the growing availability of 3-D printing technology makes it cheaper and easier for data thieves to target customers at a business' physical point of sale, allowing for the quick creation of skimming devices (which fit over legitimate credit card readers to steal card data) and shimming devices (which fit inside card readers). Incidents of compromised ATMs and merchant devices rose 30% from 2015 to 2016, following a six-fold increase in 2015.[3]

> "Fraud isn't going away—it's getting more sophisticated."

After stealing personal and credit card data with these methods, criminals sell it to be used in card-not-present fraud. Such black-market data sales also have become more sophisticated. For example, cybercriminals bundle stolen credit card information from a single zip code and sell it in that area to evade security systems that monitor out-of-area credit card use.

### THE PUBLIC AND PRIVATE COST OF A DATA BREACH

Businesses incur a range of expenses when data breaches occur, including refunds for fraudulent purchases, penalties for noncompliance with EMV chip card standards and reimbursing credit card issuers for the cost of replacing cards, which can run more than $200 apiece.

Moreover, insurance companies after a breach may demand that businesses hire outside legal counsel or breach coaches to oversee security. (Cases where 30,000 or more cards have been compromised typically trigger such requirements.) Larger companies may also need to invest in a PCI forensic investigator to help pinpoint where the breach happened and prevent future attacks.

Merchants with compromised data also incur considerable public relations costs.

"Customers lose trust in a business after a breach," says Gregg Kambour, vice president of solutions consulting at Bank of America. "Canceling and replacing cards is directly disruptive to customers' lives."

Companies may have to hire PR firms to handle public announcements about the breach and to develop and execute campaigns to win back public trust. The expenses can add up quickly: Simply hiring a PR agency can cost $100 to $500 per hour, depending on the size of the firm. Putting the agency on retainer can cost from $1,000 to tens of thousands of dollars per month. Add the costs of direct mail campaigns, traditional and social media outreach and increased customer support, and the sums can reach staggering levels.

## EVOLVING SECURITY SOLUTIONS

Security threats evolve constantly, as do technology solutions.

"EMV is not a cure-all," says Brennan. Pair it and data encryption with tokenization to protect customer data further. Tokenization—which retrieves credit card data using randomly generated one-time tokens that carry no personal information—enables companies to remove credit card data from their internal networks.


"Technology companies like Bank of America Merchant Services are trying to provide a holistic view of fraud activities to beat down both card-not-present and card-present fraud," says Raoul Aranha, vice president, Security, Fraud and Analytics Services at Bank of America Merchant Services.

For example, security companies are:

- Developing machine learning systems that can track fraud before it occurs. Machine-learning software combs through company and online data to identify characteristics of fraud automatically. It looks for patterns in credit card use, identifies anomalies in those patterns and flags the anomalies as potential fraud activity.
- Building broad networks that share data on fraud. "Bank of America Merchant Services has access to issuer data, network data and merchant-acquiring data," says Michael Roberts, chief marketing and digital strategy officer at BAMS. "That allows us to create models that will outperform company models that rely solely on internal data." These networks can alert merchants that a card making a purchase triggered a red flag at another retailer.

## PROTECT YOUR BUSINESS—AND YOUR CUSTOMERS—GOING FORWARD

Holding ongoing conversations about new developments with security providers and payment vendors, such as Bank of America Merchant Services, can help businesses apply emerging technologies that suit their size, industry and customer base. But a few basic preventative measures from within can help thwart data theft attempts. Here are two:

- Teach employees at the point of sale to search for skimming and shimming devices by looking for ill-fitting card reader covers at the beginning of every shift.
- Run training exercises and drills—covering scenarios such as a phishing attempt—so all employees are familiar with fraud tactics and alert to them, and know the roles they are expected to play.

Every company today must safeguard customers' data in the face of constant and evolving threats. Payment technology vendors are in a unique position to help overcome that challenge. Discussions and check-ins with your payments and security solution provider can help you stay on top of today's data threats and how to stop them, so you can focus on growing your business.

Bank of America
Merchant Services

For more information on how Bank of America Merchant Services can help you optimize your business and customer experience through integrated security and fraud solutions, call your Bank of America Merchant Services business consultant or 855.833.3614. We're here to help.

[1] Javelin, "2017 Identity Fraud: Securing the Connected Life," 2017. https://www.javelinstrategy.com/press-release/identity-fraud-hits-record-high-154-million-us-victims-2016-16-percent-according-new

[2] Juniper Research, "Online Payment Fraud: Emerging Threats, Key Vertical Strategies & Market Forecasts 2017-2022," 2017. https://www.juniperresearch.com/press/press-releases/retailers-to-lose-$71-bn-in-card-not-present-fraud

[3] FICO, "Fico Reports a 70 Percent Rise in Debit Cards Compromised at U.S. ATMs and Merchants in 2016," 2017.



LC-BB-CBB-BAMS-WP-Fraud is Evolving Insight-ARHSJMPH-10/2017