Testimony of Todd McCracken
President and CEO

House Committee on Small Business Hearing:

"Small Business, Big Threat: Protecting Small Businesses from Cyber Attacks"

April 22, 2015

Good afternoon. My thanks to Chairman Chabot, Ranking Member Velazquez and the members of the Small Business Committee for inviting me to testify today on the impact of cybersecurity and credit card fraud issues on the health and growth potential of millions of small businesses.

My name is Todd McCracken, and I am President and CEO of the National Small Business Association (NSBA)—the nation's first small-business advocacy organization. NSBA is a uniquely member-driven and staunchly nonpartisan organization. NSBA has members in all sectors and industries of the U.S. economy from retail to trade to technology—our members are as diverse as the economy that they fuel. Small employers comprise 99.7 percent of all employer firms in the U.S. One in two workers in the private workforce run or work for a small business, and one in four individuals in the total U.S. population is part of the small-business community. Those are certainly impressive figures.

In the last few years, cybersecurity has emerged as a significant problem and concern for the small-business community. By the end of 2014, according to NSBA's Year-End Economic Report, fully half of small businesses reported having been the victim of a cyber-attack (up from 44 percent in 2013). Of those, 61 percent say an attack had occurred within the last year.

Cyber-Attacks on Small Businesses are Becoming More Prevalent

While a 14 percent increase in the number of small-business victims of a cyber-attack is significant, we believe the real story is the increasing impact those attacks are having on small businesses, in terms of both the interruption of normal business operations and the direct financial cost of the attack.

In 2013, only 12 percent of businesses reported that resolution of the cyber-attack required more than one week; by late 2014, more than one in five such attacks were still unresolved after one week, with 13 percent of them requiring more than two weeks. Three in five businesses experienced a service interruption, and a third had their websites go down for some period.

Small Companies Have Fewer Resources to Deal with Cyber-Attacks

Many small companies are not in a position to have a dedicated IT department, and many either outsource IT functions or assign such duties to an employee with other responsibilities—often the owner him/herself. In fact, the number of business owners who personally handle IT support appears to be on the rise. When we asked in 2010, 25 percent of business owners indicated that they were primarily responsible for IT support in their companies, while a larger number (36 percent) said they contracted with an outside vendor. By 2013, those numbers had essentially reversed, with 40 percent of business owners handling IT personally and only 24 percent indicating that they outsourced the function.

In the case of an outsourced IT function, a very small business might not be high on the IT firm's priority list of clients, even though such a firm is more likely to have the experience and technical expertise to resolve the issue quickly. In the case of in-house functionality, new issues might require research and training, making mistakes and delays more likely. In either scenario, dealing with the technical side of a cyber-attack presents unique challenges to our smallest companies.

Cyber-Attacks are Becoming Much more Costly

Perhaps the most startling finding of our most recent cybersecurity data was the sharp increase in the direct financial cost of cyber-crime on small companies. Of those companies reporting some kind of cyber-attack, the *average* amount of

money stolen from a bank account rose from $6,927 in 2013 to $19,948 by late 2014, a 188 percent increase in a short amount of time.

This dramatic increase in stolen funds appears to be related to a sharp rise in the incidence and sophistication of so-called phishing scams. These scams send emails closely mimicking those of banks or other trusted institutions and citing an urgent need to login to an account or provide some other vital information. Small businesses are particularly vulnerable to these attacks, since multiple employees could have access to vital information. Further, business accounts do not enjoy the same level of protections and guarantees against loss and theft as those provided to consumers—a reality that many small-business owners do not discover until it is too late. Consumers are protected by Regulation E, which dramatically limits their liability in a cyber-heist. Commercial accounts, however, are covered by the Uniform Commercial Code (UCC). The UCC does not hold banks liable for unauthorized payments so long as "the security procedure is a commercially reasonable method of providing security . . ." Few small businesses that are the victims of theft from their bank accounts ever recover those funds.

According to Verizon's 2015 Data Breach Investigations Report, phishing has increased dramatically in just the last four years, having gone from about 2 percent of cyber-attacks in 2010 to over 20 percent in 2014. Moreover, these phishing attacks have become much more sophisticated, with a high degree of verisimilitude. Small companies need to engage in ongoing employee training to recognize and avoid these dangerous traps.

Credit Card Fraud and Small Businesses

Various forms of credit card fraud have been part of our financial landscape for some time. However, the increased technical prowess of cyber-thieves—and the continued prevalence of magnetic stripe cards—has taken credit card fraud to

heightened levels. The U.S. finally appears to be taking significant steps toward the introduction chip (EMV) enabled cards, or so-called chip and PIN cards.

Liability Shift

As EMV cards begin to enter the U.S. market, the credit card issuers will begin to shift liability for card fraud to the entity with the lowest level of security. The practical effect of this rule—effective Oct. 1, 2015—is that merchants will, for the first time, become liable for fraudulent card use if they have not upgraded to the latest EMV card reader technology and software.

This move to EMV means that millions of countertop card readers will need to be replaced. The change is also likely to mean new software and a need for employee training. Therefore, since the transition will both be expensive and time-consuming, smaller merchants should carefully consider whether the shift to EMV card readers makes sense for their businesses, at least for now.

Merchants who sell low-priced goods and consumables, for instance, are unlikely to be targets for credit card fraud, so they are unlikely to see their potential liabilities significantly rise as a result of the shift. However, merchants that sell more expensive goods with strong re-sale value (e.g., electronics, jewelry), and who do not know their customers well, have a higher incentive to move to EMV card readers. Small businesses should carefully examine their own "charge-back" history to determine whether the investment in the new technology and processes makes sense for them at this time.

Hastening the Transition to a More Secure EMV Environment

Besides a general lack of awareness of the liability shift issue, there are two other major reasons that smaller merchants have not generally made the switch to EMV card readers:

1. Card issuers are not offering reduced interchange fees for merchants using EMV care readers, despite promised reduction of fraud resulting in their use. Given that card issuers have long blamed fraud as a prime cause for high interchange fees, merchants will naturally expect that EMV implementation will drive down those fees.

2. Card issuers have not yet made their own transition to EMV cards. Until smaller merchants see a market demand (in the form of their customers using chip-enabled cards), they are unlikely to move quickly to accommodate a non-existing demand.

Stepped-up issuance of EMV-enabled cards, combined with the eventual elimination of magnetic-stripe cards altogether is the only logical path toward a significant and lasting reduction in card-based fraud, at least for "card-present" transactions.

Recommendations

Cybersecurity is a large and growing threat to the small-business community. NSBA urges Congress to move forward on establishing streamlined guidelines and protocols to ensure the protection and security of online data and financials, but cautions against a knee-jerk reaction that would unfairly place a disproportionate burden on America's smallest firms:

- Legislation to enhance America's cybersecurity should provide clear, simple steps for companies to follow when their data is breached and must balance the need for greater information sharing with privacy rights.
- Any federal discussion on cybersecurity or development of a private-public partnership or advisory board must include representatives of small business.

- Extend consumer banking protections to the banking accounts held by America's smallest firms.
- Congress should maintain oversight on the credit card technology transition and ensure small firms are protected against any unfair or seriously burdensome costs or liabilities associated with transitioning to the new technology.

Conclusion

Thank you for the opportunity to speak with you today. I hope that we can work with each of you as we advance to solutions to the significant cybersecurity issues before us.