First Annapolis®
Consulting | M&A Advisory Services

Executive Interview Series

A Supplement to the First Annapolis Navigator

A Conversation with Maddy Aufseeser, CEO and Co-founder Tender Armor, LLC

In this conversation, Maddy Aufseeser, CEO of Tender Armor focuses on credit, debit, and prepaid card fraud prevention and security trends. Tender Armor is a SaaS technology company. The firm's inaugural solution is CVV+, that protects bank issued payment cards from fraud in the growing card-not-present (CNP) transaction segment. The company tag line "make it secure, keep it simple" captures the company's essence: providing easy-to-use real-time industry services that primarily protect not-in-person monetary transactions from fraudsters.

Focusing on large scale high velocity money movement and payments, Tender Armor meets the needs of financial services, insurance, and government entities. The Tender Armor team is comprised of proven payment industry veterans, and engineers.

Maddy Aufseeser has over 30 years of experience in banking and payments with expertise in the credit, debit, and prepaid card markets. She is a trusted advisor to senior leadership teams and staff at a long list of Fortune 500 companies in the FI sector. In just the past year, she has been recognized by BankInnovators.net as a 2016 top innovator to watch shaping the future of banking and by Remodista as a 2017 Women-2-Watch in retail disruption.

1. **What unmet need or insight into the future of the market did you see that drove you to create Tender Armor?**

   Escalating fraud, increasing consumer concerns, and growing online shopping trends have simultaneously converged. These market dynamics created an unmet need for simple, easy-to-use, consumer controlled, fraud prevention tools. The advent of EMV chip cards around the world pushed fraud to the least protected CNP shopping channels. Consumer worries grew as media outlets drew attention to hacks, breaches, and fraud events. All the while, consumers have little knowledge, means, or tools available that protect their credit and debit cards when shopping online or over-the-phone. Meanwhile, financial institutions are still primarily dependent on detection based fraud systems and merchant mitigation attempts in the face of swelling losses and fraud related expenses.

   Tender Armor was created in anticipation of these converging market forces. The company saw a market void and a global opportunity to offer effective prevention tools that authenticate consumers, not just a device or card. The company has two primary goals for its inaugural product CVV+:

   1. Providing FIs with a payment card fraud prevention tool that reduces losses and expenses for all cardholders, any way and anywhere consumers shop, without relying on merchants.
   2. Providing consumers with the security they want with the features they need. In today's global marketplace, the cardholder does not know what a merchant or a bank has done to protect a payment card transaction. Giving the consumer the control deputizes the cardholder, which alleviates rising fear about the safety and security of their payment cards. Preventing fraud also relieves the cardholder from the hassle of dealing with the bank once fraud has occurred.

2. **What are the roles of (and benefits to) the issuer, consumer, and merchant in a CVV+ transaction?**

   Offered to FI card issuers and their providers across the globe, CVV+ creates an extra layer of security to credit, debit, and prepaid cards primarily used in card-not-present transactions and some POS transactions. CVV+ works by replacing the static security code on the face of the card with a dynamic, out-of-band, code that authenticates the cardholder. FIs can quickly and easily add CVV+ to any existing payment card – without card reissues.

   The CVV+ solution works in the existing eco-system. The solution is transparent to the merchant – without requiring any merchant intervention or changes to their websites. Consumers choose when, how, and how often they want to receive their personal CVV+ code, which fits securely within the cardholders' lifestyle.

   CVV+ saves FIs from costly write-offs, card replacements, and servicing expenses. By deploying CVV+ and preventing fraud, FIs can reduce the possibility of false-positive declined transactions often caused from detection solutions. By preventing fraud with CVV+ FIs also stem the risk of cardholder attrition, reduced card usage, or replacement cards relinquished to the bottom of a desk drawer after a fraudulent event.

3. **What do you see as the most significant fraud threat to financial institutions today and as the market evolves?**

   The two companion trends that are particularly alarming for FIs are (1) the lost revenue from post fraud cardholder behaviors and (2) the lack of knowledge around the total cost of fraud.

   The fact is that fraud changes the cardholder's behavior. Studies conducted by the U.S. Department of Commerce, American Express, and our own 2016 independent research, all reported significant changes in cardholder behavior once fraud has occurred. The studies agree that more than half of all cardholders affected by fraud use their replacement card less or close their account, costing FIs untallied numbers of transactions, customers, and subsequent revenues. Additionally, both

the American Express study and the Tender Armor study indicated that more than 65% of U.S. consumers are willing to use a security feature to prevent fraud on payment cards, suggesting this is a feature consumers want.

Despite FIs best intentions most FIs do not calculate the total cost of fraud on a portfolio. Nor do FIs typically know all the portfolio implications inclusive of the hit on profitability and margins. This is because of the way FIs are typically organized, the specific attention to fraud dollar losses, and the way cardholder behavior is analyzed. While FI departments do collaborate on many fronts, they do not collect data and attack all the fraud impacts across business areas in a coordinated fashion. For example, risk departments monitor fraud losses but not all the other associated fraud expenses because the risk departments may not have a stake or view into the other aspects of the business. These expenses such as card replacement costs and customer servicing add up quickly. Product groups measure cardholder behaviors such as reduction in card usage, and cardholder attrition. Yet, product groups don't consistently or adequately measure cardholder behavior before and after a card has been compromised. Since risk groups, product teams, and customer service organizations in FIs tend to be siloed, there is little or no cross functional analysis done that accounts for all the fraud related expenses together to paint a cohesive total cost of fraud picture.

Fraud impacts servicing expenses, attributes to cardholder attrition, lack of card usage, and can be just as costly as the fraud dollar losses. The recent 2016 Federal Reserve Board of Governors biannual debit card interchange report suggests how big the loss problem is. Report findings indicate debit card fraud losses grew across all categories by 44% in 2015 from 2013. Average fraud losses per CNP transaction grew to $58 in 2015 with issuers paying 28% of the bill equaling $16.24 per incident. Once an FI knows fraud losses and downstream implications, they can start understanding the other costs. For example, the cost of fulfilling an EMV replacement card can add an average of $4.00 per reissued card to the fraud costs, a 25% increase in cost. This one example demonstrates how quickly the total cost of fraud balloons when adding in other fraud related expenses. Imagine the total fraud cost when attributing lost revenues from reduced card usage, and cardholder attrition.

FIs are missing an opportunity to improve the customer experience and portfolio margins by not monitoring and accounting for the total cost of fraud. Monitoring and measuring efforts should be inclusive of accounting for fraud's impact on the portfolio, be it attrition or card usage. Most FIs are content when fraud losses are kept within industry standard ratios. That may be a myopic view when considering fraud prevention methods can help eliminate costly unnecessary expenses, preserve cardholders, card usage, and enhance portfolio profitability. Therefore, FIs should work toward understanding the total cost of the fraud not just the dollar losses.

4. **How is CVV+ different from other card not present fraud solutions? Does the product work in conjunction with other services or does it act as a replacement?**

   The CVV+ solution works to authenticate the cardholder and not a singular specific device or card. CVV+ has four essential elements combined that make it unique, these four service features are:

   1. *Omni-channel solution* - consumers can use CVV+ the same way across all the primary purchasing channels (e-commerce, m-commerce, phone orders, and POS)
   2. *Form factor agnostic* - CVV+ works with any payment method (physical cards, virtual cards, computers/laptops, mobile devices, and tablets)
   3. *Card type and brand agnostic* – can work on every card in the market today without reissues; any card type (credit, debit, prepaid, and commercial cards) and with any brand (American Express, Discover, MasterCard, Visa)
   4. *Issuer and cardholder configurable options* such as the CVV+ code delivery method, the code rotation frequency, and the ability to have multiple cards tied to one CVV+ code

   CVV+ can work seamlessly in conjunction with other fraud solutions. As an example, CVV+ usage can be included in detection risk scoring models as an add-on to reduce false-positive declined transactions.

5. **What are the implementation requirements associated with CVV+ – what is the typical timing and the integration effort?**

   Tender Armor offers three different CVV+ integration methods to suit client needs. The SaaS Web API model is the most preferred method, being the easiest to install, and taking the least amount of time to get up and running. CVV+ can be installed and operational on a card issuing authorization platform in less than 30 days, including testing. Web API integration means Tender Armor handles all data, software, hardware maintenance and updates on a secure, dedicated, high-performance, high-availability cloud architecture system complete with redundancy for fail-over and disaster recovery.

U.S. Headquarters
Three Park Place, Suite 200
Annapolis, Maryland 21401, USA
U.S. Office +1 (410) 855 8500
www.firstannapolis.com

Europe Office
Keizersgracht 313-I
1016 EE Amsterdam, The Netherlands
Europe Office +31 (0) 20 530 0360
info@firstannapolis.com