A Tender Armor Company

Competitive Landscape 2016

Fraud Prevention Solutions

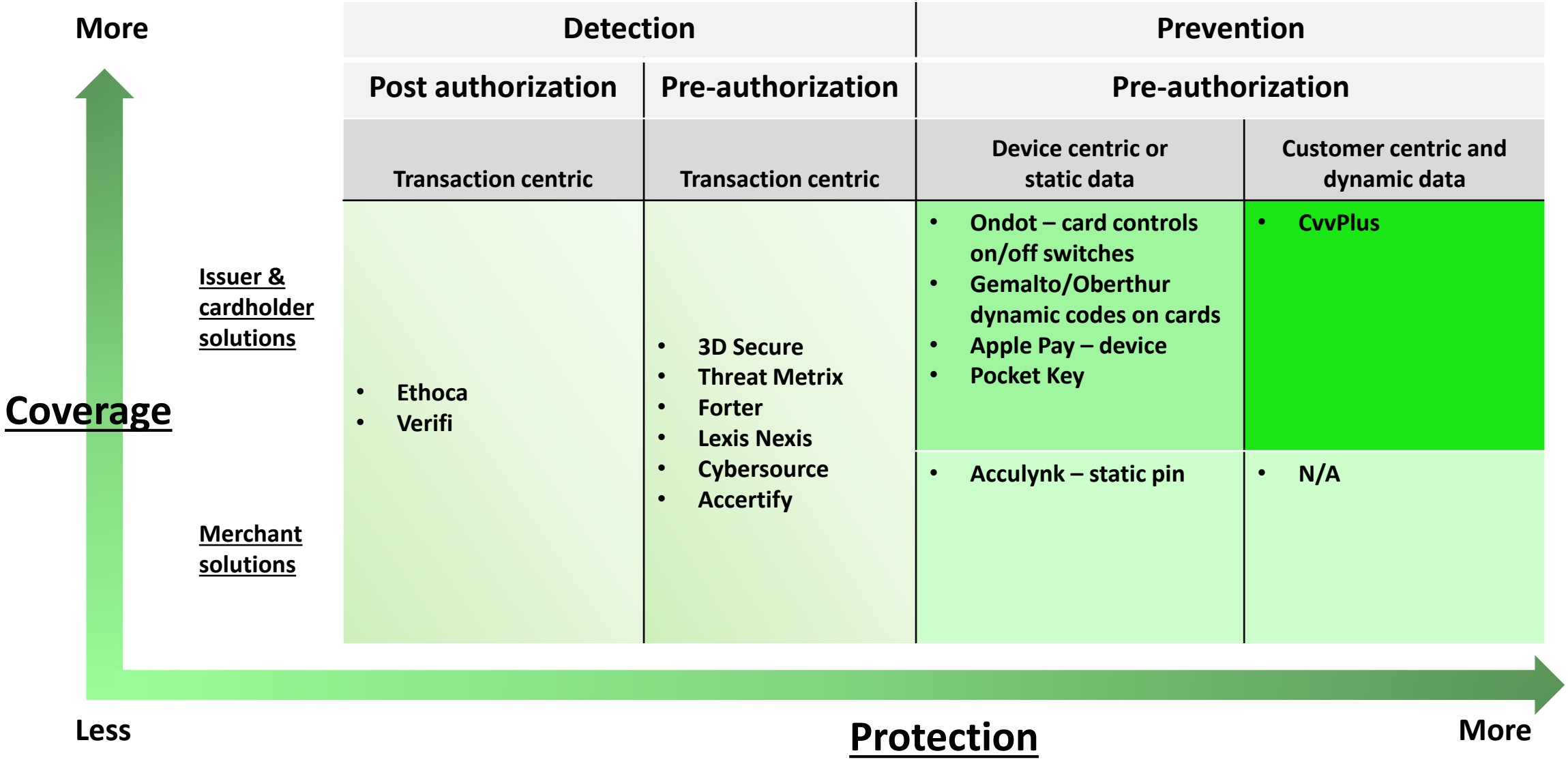
Make it secure, keep it simple!

An ounce of prevention more effective than curing the problem – market overview

- Many different solutions on the market target an array of constituents, utilizing varying approaches to solve different parts of the fraud problem
  - Constituents can be segmented in three primary groups:
    - Merchants
    - Bank issuers
    - Cardholders
  - Solutions utilize varying techniques and solve for fraud at various points in the transaction and can be classified in four categories and two high level groupings:
    - Detection solutions:
      - Pre-authorization that protect a specific transaction
      - Post-authorization detection solutions that aim to minimize chargebacks
    - Prevention solutions:
      - Pre-authorization solutions authenticating a “form-factor” (a device, or payment card) and/or relying on static data
      - Pre-authorization solutions that authenticate a specific person utilizing dynamic data
- The highest level of protection is achieved when the problem is solved through prevention and is holistic:
  - Act to prevent fraud before it occurs rather than detect fraud during a transaction
  - Aim to authenticate the actual cardholder not just a specific transaction, individual device, or particular merchant
  - Work across many transaction types, such as online, mobile, phone and POS
  - Operate dynamically and independent of the card account information

CvvPlus is the only solution in the market that currently meets these criteria

Fraud solution market landscape diagram



Market Situation - CvvPlus Focuses on Prevention, Compliments Existing Products, and Fills Market Gaps

Feature	CvvPlus	Dynamic Security Code Cards	Pocket Systems	3D Secure	Acculync	Cybersource & Accertify
Protects CNP transaction from clearing authorization if the card is lost, stolen, account take-over, or compromised and not reported	✓					
Supports CNP phone transactions not just online	✓	✓	✓			
Consumer controlled product vs. merchant controlled	✓	✓	✓			
No merchant integration required	✓	✓	✓			
Supports any card type	✓	✓	✓	✓		✓
Supports multiple cards and card types in a single installation	✓			✓		✓
Preventive vs detective	✓	✓	✓		✓	
No special device required	✓			✓	✓	✓
Methodology detached from card, account, & PCI data	✓					
Works on existing cards in market	✓			✓	✓	✓
Works during transaction without API call out to third party	✓					

3D Secure – a closer look: limitations and vulnerabilities

Comparison points	3D Secure	CvvPlus
Required constituent adoption	**Merchants, issuers and consumers:** If a merchant is not using 3D secure than the issuer's cardholder is not protected (no adoption, no coverage), there will never be 100% 3DS adoption by all merchants which means banks are still vulnerable	**Issuers and consumers:** CvvPlus is transparent to merchants and does not require the merchants to adopt the service or change anything about the way they accept or process a transaction
Transaction types	**Online only:** 3 D Secure does not work for phone orders representing 20% of all CNP transactions in the US and higher in Europe even higher fraud dollar volumes	**Online, phone, mobile, and POS:** In addition to transactions such as online, CvvPlus supports phone orders and can function as a dynamic PIN replacement at the POS. Additionally, CvvPlus has other use cases such as call center cardholder authentication
Authentication target	**Pre-authorization detection on specific merchant transaction:** If the consumers' merchant online account is hacked, the fraudster can start transacting because the card is already stored on file. 3D secure only authenticates the transaction not the consumers' merchant accounts or consumers themselves	**Pre-authorization dynamic cardholder prevention:** CvvPlus authenticates the cardholder so if an individuals merchant or bank account is hacked and the security code printed on the card is entered and not the CvvPlus code the transaction will get declined
Static vs. dynamic data	**Static data for authentication:** If that data gets compromised again there is a potential exposure problem	**Dynamic data:** CvvPlus uses a dynamic code that can change as frequently as the bank or cardholder wishes
Coverage	**5% of online transactions evaluated:** Decision to evaluate based on risk criteria, then a possible stepped-up cardholder question may be used during the transaction	**All transactions when the card security code is requested:** No other cardholder action required
Interchange and liability shift	**Favors the merchant:** 3DS creates a liability shift for the transaction reducing interchange rates merchants pays and reduces revenue bank card issuer receives. Subsequent fraudulent transactions become issuer responsibility (for any reason: account take over at the merchant and "friendly" fraud are two examples) and absorb the costs	**No change:** Issuers maintain interchange income at current rates and have no more or less liability responsibility