شرکت خدمات انفورماتیک

# اهمیت نهانش(توکن کردن)برای تامین امنیت زنجیره پرداخت

**نوش داروی آسیب پذیری های پرداخت کارتی نیست EMV**

Andras Cser, Ed Ferrara, and John Kindervag

**مدیریت سیستم های نوین بانکی**
**ترجمه: فاطمه مرادی**

## چرا این گزارش را بخوانیم؟

آیا کارت اعتباری به زعم مشتریان آمریکایی مرده است؟ با رخداد های اخیر رخنه های داده انبوه در کارت اعتباری در خرده فروشانی مثل Target , Home Depot دیگر وقت آن شده است که صنعت پرداخت بالغ کنونی، تغییر بکند. در این گزارش برای ترسیم آینده بازار پرداخت در آمریکا تعداد زیادی از متغیر ها شامل:

داده های زیادی از اطلاعات مشتریان در شعب ،

قانون تغییر مسئولیت پرداخت در اکتبر 2015 ،

میزان امنیت موبایل Europay و مستر کارت و ویزا و

پرداخت های غیر لمسی EMV

و رسیدن درصد نفوذ دستگاه های موبایل به بالای 72 درصد

مقایسه شده اند و کمک خوبی به گروه و متخصصان امنیت و ریسک است. فارستر پیش بینی میکند که با ایجاد امنیت و رمز نگاری و تراکنش های بر اسا س توکن بر روی کیف پول های دیجیتالی و کارت های NFC و پرداخت های غیر لمسی EMV باعث شده است که اینها رقبای جدی برای EMV chip and signature و chip and pin payment در آمریکا باشند. و همچنین پیش بینی میکند که EMV های پلاستیکی تا سال 2020 پذیرش جدی در آمریکا نخواهند داشت.

## پرداخت های امن جز اصول اساسی برای رشد مشتریان و نگهداری انها میباشد

فارستر پیش بینی میکند که تا سال 2019، 142 بیلیون دلار پرداخت های موبایلی انجام میشود.( شکل 1) اطمینان و اعتماد مشتری باعث پذیرش آنها در این شکل جدید پرداخت میشود. در هنگام پرداخت با دانستن شماره PII او ( مشابه شماره ملی در ایران) اطلاعات کارت پرداخت او و عادات خرج کردنش اطلاعات خوبی برای هوش تجاری در اختیار ما میگذارد. و چنانچه مشتریان شما نتوانند در مسئولیت نگهداری این اطلاعات حساس، به شما اعتماد کنند، جذب رقبای شما خواهند شد. بنابراین مقوله امنیت و ریسک یکی از مولفه ای اصلی نگهداری و خدمت رسانی به مشتری میباشد. مشتریان انتظار دارند که در زنجیره پرداخت اطلاعات شخصی و پرداختی آنها حفظ شود. روند های کنونی نشان میدهند که:

- **هک کردن تکنولوژی پایانه های فروش کنونی بسیار ساده است.** در سال 2014 رخنه اطلاعاتی عنوان بسیاری از سر فصل های اخبار بود. رخنه اطلاعاتی بسیار هزینه بر بودند. بسیاری از آنها در برهه ای بدون اینکه مشخص شود باعث از بین رفتن اطلاعات مشتریان میشدند. تکنولوژی POS ها قدیمی و درجه امنیتی کم است و معمولا سیستم عامل آنها XP است که دستیابی به شماره کارت ها را برای هکر راحت میکند.
- **هزینه های نقص داده سر سام آور است.** Home Depot حدود 43 میلیون دلار در سه ماهه گذشته صرف نقص داده کرده است. یا شرکت Target مبلغ هنگفت 148 میلیون دلار را صرف جبران تاثیرات رخنه اطلاعاتی درکارت های اعتباری خود کرد. این هزینه ها کاملا اجتناب ناپذیر اند و به نوعی هشداری برای توجه به تکنولوژی امنیت هستند. و اگر از رمز نگاری و یا توکن کردن استفاده کرده بودند این هزینه های رفع نقص قطعا کاهش می یافت.

- **رسوخ امنیتی از بالاترین تا پایین ترین سطح خرده فروشان را تحت تاثیر قرار میدهد.**

مطالعه اخیر نشان میدهد که 44 درصد رخنه اطلاعاتی و 60 درصد دزدی اطلاعات رخ داده است.45 دردصد خریداران به خرده فروشان در نگهداری اطلاعات اعتماد ندارند. و بعد از یک رخنه اطلاعاتی 12 درصد خریداران دیگر از خرده فروشان خرید نکردند و 36 درصد کمتر خرید کرده اند.و 79 درصد آنهایی که به خرید ادامه دادند پول نقد را به کارت ترجیح میدهند و آمار نشان میدهد در خرید نقدی معمولا پول کمتری خرج میشود.

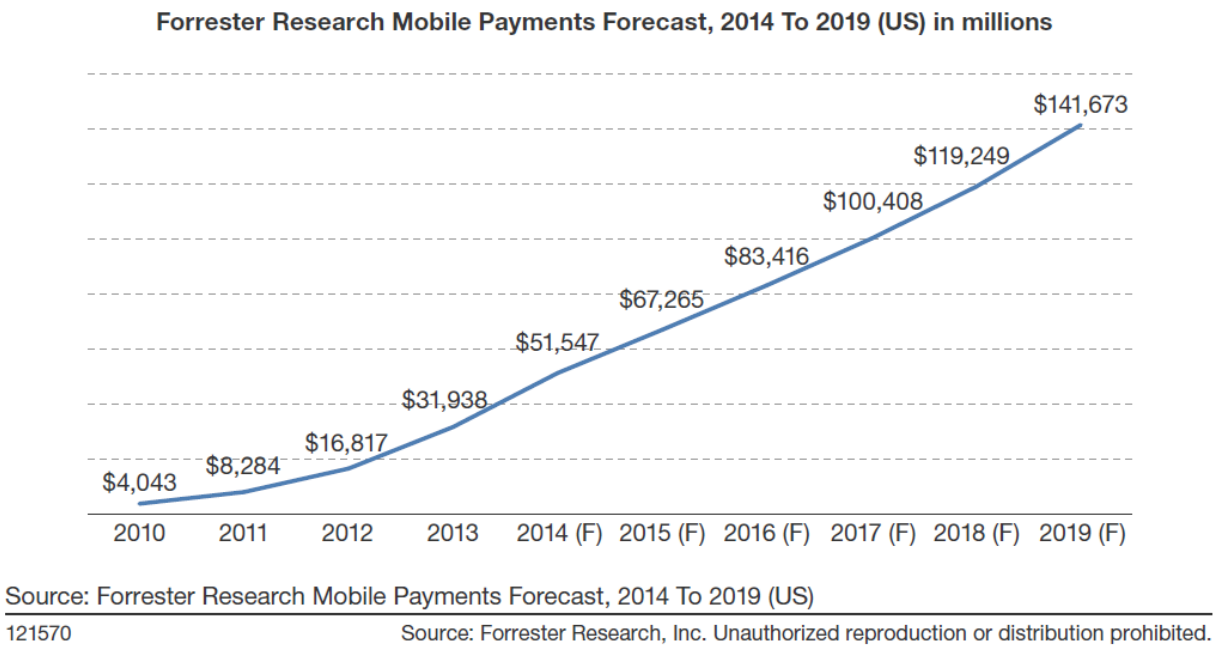
- **موبایل ها امنیت ارتقا یافته خوبی ارائه میدهند.**

زیر ساخت پرداخت کنونی برای 50 تا 60 سال پیش که با کارت های مغناطیسی خرید میشد طراحی شده است. برای پرداخت های امروزی نیاز به تکنولوژی های جدید تر و احراز هویت قوی تر و مقاوم سازی کل سیستم پرداخت میباشد.
شکل های جدید امنیت پرداخت مثل (Starbucks Card) نه تنها امنیت بهتری فراهم میکنند بلکه مزایای تطبیق پذیری نیز برخوردارند.

- **تجارت الکترونیک به سمت برتری و نمایان شدن پیش میرود**

فارستر انتظار دارد فروش انلاین در آمریکا در سال 2014 به مرز 297 بیلیون برسد و یا حداقل به 9 درصد تمام فروش ها در امریکا برسد. بازگشت خالص سرمایه در یک بازه زمانی مشخص (CAGR) از 11.1 درصد در بین سال های 2013 و 2018 به یک بازده 444 بیلیونی در فروش آنلاین تا سال 2018 برای نجارت الکترونیک آمریکا یش بینی میشود . که در این میان امنیت پرداخت آنلاین و تراکنش های بدون حضور کارت مهم میشود.

شکل 1 جدول رشد سود در آمریکا




Source: Forrester Research Mobile Payments Forecast, 2014 To 2019 (US)



## توکن کردن باید یک اصل اساسی در اکوسیستم پرداخت امن باشد

در حالیکه تکنولوژی ها ی پرداخت یک رخنه های امنیتی ذاتی دارند ولی در عین حال کنترل های امنیتی پیشرفته ای ارائه میکنند. شکل 2 و 3 را ببینید. در مقابل بسیار ی از بخش های صنعت ما را به این باور رساند که EMV یک راه حل جامعی برای تمام مسائل امنیتی نمیباشد. دلایل زیر برای این مسئله مطرح می شوند:

- **در حالیکه EMV دستکاری را تقریبا غیر ممکن میسازد ،کپی کردن کارت با نوار مغناطیسی بسیار آسان است** اگر پیشخدمت رستوران کارت شما را از جلوی چشم شما دور کرد میتواند کپی کاملی از اطلاعات شما داشته باشد و شما تا زمانی که صورت حساب بگیرید و در ان مبلغی از شما بابت تغییر اطلاعات کسر شده باشد متوجه نخواهید شد. کارت های پلاستیکی EMV از یک چیپ برای صحت کارت برای تایید خرید استفاده میکنند که کار را برای کارت های جعلی(دستکاری شده ) به نسبت کارت های نوار مغناطیسی مشکل تر میکنند.

- **EMV به خودی خود نمیتواند از رخنه اطلاعاتی جلوگیری کند مانند آن که برای Target پیش آمد**

EMV بدون توکن کردن شماره کارت و تاریخ انقضا را که در طول تراکنش جا به جا میشوند رمز نگاری نمیکند. EMV یک سر و گردن از تکنولوژی های کارت کنونی جلوتر است چون چیپی دارد که مانع جعل است اما همچنان جلوی جعل خود کارت را نمیگیرد (به عنوان مثال شما میتوانید اطلاعات را کپی کرده و یک کارت نوار مغناطیسی که با همه ترمینال های مغناطیسی کار میکند بسازید) و یا استفاده آنلاین جعلی از کارت در تراکنش های بدون حضور کارت را نیز نمیتواند جلوگیری کند.

- **استفاده از رمز نگاری و توکن کردن بدون EMV هم از نفوذ جلوگیری میکند.**

رمز نگاری مستلزم بدست آوردن شماره کارت توسط ترمینال POS قبل ارسال در هر جایی از شبکه پرداخت میباشد. مراحل توکن کردن به این شرح است: مرحله اول با اولین تراکنش توسط مشتری جدید ، پایانه POS شماره کارت رمز شده را به سرویس توکن کردن PCI-DSS میفرستد . بعد از آن در مرحله دوم سرویس توکن کردن با یک شناسه انرا در پایگاه داده مینویسد که شماره کارت را به نام پذیرنده کارت آدرس شماره تلفن و سایر اطلاعات پیوند میدهد. سپس در سومین مرحله کار احراز هویت به شکل عادی از طرف فروشگاه(پذیرنده) انجام میشود . در مرحله چهارم یک توکن ( و نه خود شماره کارت) را به فروشگاه(پذیرنده) برمیگرداند. که تایید تراکنش پرداخت است. برای پرداخت های متعاقب و بعد از این فروشگاه(پذیرنده) تنها توکن ( و نه شماره کارت ) را میفرستد و مرحله سوم به بعد انجام میشود.

شکل 2 آسیب پذیری های متد های پرداخت

| NFC غیر لمسی دستگاه های موبایل | EMV NFC غیر لمسی | EMV لمسی | نوار مغناطیسی |
|---|---|---|---|
|  |  |  |  |
| • شنود رادیویی ( با اسکن تماسی) اطلاعات کارت میتواند با اسکنر مجاور با "خواندن" اطلاعات کارت دزدیده شود. | • آسیب پذیری مشابه کارت تماسی EMV<br>• شنود رادیویی ( با اسکن تماسی) اطلاعات کارت میتواند با اسکنر مجاور با "خواندن" اطلاعات کارت دزدیده شود. | • به مانند کارت های مغناطیسی به شنود حساس هستند به همان نسبت به شنودهایی که توسط POI/keypad و سیستم عامل و شبکه PA میباشد<br>• کارت های EMV که در آمریکا گسترش یافته اند همچنان یک نوار مغناطیسی دارند تا با | • کد خطاهای برنامه پرداخت PA<br>• توافق POI و مصالحه keypad/PIN (تمپر کردن دستگاه ها ، لاگ کردن ، هک کردن درگاه های COM)<br>• خراب شدن حافظه سیستم عامل<br>• اسکن کردن فایل سیستم |

| | | | |
|---|---|---|---|
| | | قدیمی ها تطابق داشته باشند که به کلاهبرداران اجازه میدهند از اطلاعات کارت تقلب بدون حضور کارت انجام بدهند.<br>• رمزنگاری ضعیف توکن کردن EMV میتواند در قسمت PA رخنه داشته باشد. | عامل( Microsoft windows pagefile.sys)<br>• شنود شبکه و داده<br>• در هر نقطه ای از زنجیره پرداخت اگر شماره حساب شخصی (Pan) و دیگر موارد احراز هویت حفظ به خوبی نگهداری نشوند اطلاعات ممکن است لو بروند. |

شکل 3 مشخصه های امنیتی متد های پرداخت

| NFC غیر لمسی دستگاه های موبایل | EMV NFC غیر لمسی | EMV لمسی | نوار مغناطیسی |
|---|---|---|---|
|  |  |  |  |
| • مشخصه های مشابه به کارت های پرداخت EMV/NFC<br>• تلفن های هوشمند موارد امنیتی را با استفاده از فناوری کیف الکترونیک دارند. این موارد ذخیره چندین حساب رمز نگاری شده را امکان پذیر میسازد. | • مشخصه های مشابه کارت های EMV<br>• فناوری NFC اجازه پرداخت هایی با استفاده از امواج کارت نزدیک کارت خوان میدهد.<br>• اتصالات NFC قابل شنود اندو اگر اطلاعات بدون رمز نگاری ارسال شوند اطلاعات مشتری در خطر است. | • اطلاعات پرداخت بر روی چیپ ها رمز نگاری و توکن شده است و فروشگاه(پذیرنده) ها و کلاهبرداران توان دسترسی به داده های پذیرنده حساب را ندارند.<br>• کارت های امریکا همچنان نوار مغناطیسی را دارند که اطلاعات پذیرنده | • هیچکدام. امنیت به امنیت PA ها بستگی دارد و همچنین مراقبت کارمندان فروشگاه(پذیرنده) ها که کلاه برداری و سو استفاده ها را تشخیص بدهند<br>• اطلاعات کارت ها به صورت رمز نگاری نشده بر روی نوار |

| | | | |
|---|---|---|---|
| | | کارت بر روی ان موجود است<br>• اطلاعات مشتری در طراحی های ضعیف PA در خطر است.<br>• قوانین در اکتبر 2015 تغییر دارد و که EMV POI به جای نوار معناطیسی POI استفاده کنند به کلاهبرداران و این خرده فروشان را ترغیب میکند که تنها پرداخت هایی با کارت EMV را قبول کنند. | های مغناطیسی نگهداری میشوند. |

## چرا EMV CHIP-AND-PIN پلاستیکی در اروپا اقبال بیشتری دارد؟

کارت های پرداخت اعتباری مغناطیسی کنونی در امریکا چالش های امنیت و احراز هویت را برنمیتابند. بسیار راحت کپی و جعل میشوند و تنها در هنگام پرداخت امضای احراز هویت دارند . کارت های EMV چیپ دار در طول یک دهه بسیار در اروپا و آسیا معمول شده اند . انجمن کارت های انگلستان در یک گزارشی در سال 2011 طی گزارشی اعلام کرد که کلاهبرداری کارت های اعتباری 63 درصد افزایش یافته است. همانطور که متخصصین مدیریت کلاهبرداری میدانند که مبارزه با آنها مثل کندن سر یک مار آبی مشکل است. و پذیرش کارت های EMV توسط اروپایی ها نیز تقریبا آنرا نشان میدهد:

- **تیم های کلاهبرداری رمز را از کارت های** EMV CHIP-AND-PIN **میدزدند.** در کارت های EMV دستکاری کردن نوار مغناطیسی اگر غیر ممکن نباشد مشکل است. در نتیجه تیم های کلاهبرداری نقطه تمرکز خود را عوض کردند . بعد از اینکه کارت های EMV CHIP-AND-PIN در زنجیره پرداخت معرفی شدند.انها شروع به کپی کردن داده ها و شماره PIN ها از چیپ ها کردند و کارت های جعلی نوار مغناطیسی را تولید کردند که میتوانستند با پایانه هایی که هم نوار مغناطیسی و هم CHIP-AND-PIN قبول میکنند پرداخت انجام دهند.
- **تیم های کلاهبرداری به امریکا و تجارت الکترونیک نقل مکان کردند.** تیم های کلاهبردار عملیات خود را به آمریکا انتقال دادند و شروع به دستکاری کارت ها در ماشین های خود پرداز کردند.
- **ولی قانون تغییر مسئولیت اروپایی ها باعث شد که کارت و ترمینال های خود را بروز کنند.** این تغییر قانون باعث شد تا صادر کنندگان کارت تنها کارت های CHIP-AND-PIN را تولید کنند و باعث شد فروشگاه(پذیرنده) ها نیز پایانه هایی با زیر ساخت نوار مغناطیسی را به CHIP-AND-PIN و پایانه های غیر لمسی تبدیل کنند (در صورتی که بقیه طرف های درگیر

زنجیره پرداخت این کارت را حمایت میکردند اگر کسی از کارت های EMV CHIP-AND-PIN ÷شتیبانی نمیکرد مسئولیت کلاهبرداری با او بود)

## 1) پذیرش EMV CHIP-AND-PIN پلاستیکی تا سال 2020 در آمریکا رخ نخواهد داد

تغییر قانون ( که برای تشویق فروشگاه(پذیرنده) ها به از نوار مغناطیسی به EMV بود ) برای اکتبر 2015 برنامه ریزی شده بود با محدودیت خود پرداز ها در سال 2016 انجام میشود. قانون نظارت مالی سوخت گیرینیز 2017 انجام میشد. با توجه به محدودیت های تعیین شده زمانی پیش رو باز هم انتظار میرود که آمریکا در این تغییر ( EMV chip & pin & signature) به کندی پیش برود. بنا به سه دلیل زیر:

همه افراد درگیر در زنجیره ارزش از پذیرندگان کارت گرفته تا فروشگاه(پذیرنده) ها و پذیرنده ها processor ها و صادرکننده ها باید امنیت را در اولویت اول اهمیت قرار دهند. در ادامه مشکلاتی که افراد درگیر امدیریت ریسک ، امنیت و کلاهبرداری با آنها درگیر هستند می آوریم.

- **EMV از رخنه اطلاعاتی انبوه تعداد زیادی کارت پشتیبانی نمیکند.**

رخنه اطلاعاتی انبوه و به تبع از در معرض قرار گرفتن سایر قسمت ها هزینه ستگینی را برای فروشگاه(پذیرنده) و نه تک تک تراکنش ها دارد. و EMV هیچ حمایتی از کارت های دزدیده شده ندارد مشخصه توکن کردن EMV و فریم ورک تخصصی آن در سال 2014 تازه ارائه شدند و هنوز پذیرش عمومی پیدا نکرده است.

- **چیپ EMV بیست سال قدمت دارد. و تحت یک مقاوم سازی از نوار های مغناطیسی بود**

چیپ EMV همان اطلاعاتی را نگه داری میکند که نوار مغناطیسی دیگر کارت ها نگهداری میکند. البته EMV به صورت رمز شده نگهداری میکند. علاوه بر آن طراحی EMV برای این بوده است که قابلیتی به کارت های قبلی برای پرداخت با حضور کارت اضافه شود و برای پرداخت های بدون استفاده فیزیکی طراحی نشده است تا به این نوع کلاه برداری از آن توجه شود. البته در سال 1995 این نوع تراکنش ها بسیار کم انجام میشدند.

- **پیاده سازی های امنیت 3 بعدی هیچ زمان مورد پذیرش عمومی قرار نگرفتند** پیاده سازی های امنیت 3 بعدی (که توسط ویزا و مستر کارت و سیف کی تایید شده اند)

- **مدیریت کلاهبرداری در آمریکا بسیار پیشرفته تر است زیرا مشتریان اصطکاک کمتری تحمل میکنند.**

اولویت اول زنجیره پرداخت در آمریکا همیشه این بوده است که اصطکاک مشتری را کم کند و کار را برای آنها ساده کند. در حالیکه بانک های آمریکایی در مدیریت کلاهبرداری از عطف به ما سبق استفاده میکنند بانک های اروپایی از مکانیزم های پیش گیری کننده مانند احراز هویت دو مرحله ای استفاده میکنند. و همین تمایل آمریکا را به استفاده از EMV کم میکند. برای اینکه انها مدیریت کلاه برداری را از قبل داشته اند و آسانی کاربر را ترجیح میدهند.

## 2) پیچیدگی و بلوغ سیستم پرداخت آمریکا ترسناک است.

ساده انگارانه است اگر فکر کنیم پذیرش EMV در امریکا الگویی مشابه آن در اروپا دارد.

تفاوت زیاد این دو بازار باعث بروز نتایج متفاوتی می شود.

- **بازار پرداخت آمریکا بالغ تر و پیچیده تر از هر بازار دیگری است**

وجود classner 7500، processor و subprocessor آمریکا را تبدیل به یک بازار پرداخت بزرگ و بالغ میکند. راه حل هایی مثل ترمینال های مغناطیسی یا ترمینال های مخصوص بنزین که به صورت موروثی از قدیم بوده و استفاده شده اند میتوانند جایگزین بشوند ولی به این راحتی قابل به روز رسانی و جایگزینی نیستند.

به خاطر حجم زیاد تراکنش های کارتی و قرار داد های موقتی که بین بانک ها و شبکه های پرداخت بسته شده است وارد شدن در فضای جدید رقابتی کارت و برگشت به عقب تمام آن قرار داد ها مشکل است. American European شبکه پرداخت نمیتواند این خسارت به ازای هر تراکنش مالی را برای آمریکا جبران کند و مانند اروپا و کانادا هم مرکزی برای EMV ندارد که پشتیبانی دولتی داشته باشد و بتواند براحتی EMV را جایگزین کند.

## 3) به روز رسانی پر هزینه POS ها امکانات غیر لمسی هم میدهند.

فارستر پیش بینی میکند که پذیرش فروشگاه ها(پذیرنده) ها کلید اصلی هر روش پرداخت جدید است.از یک نقطه نظراتی پایانه ها باید حتما به روز شوند و چیپ و غیر لمسی بودن رو هر دو را بدست میاوریم. وقتی غیر لمسی بودن پشتیبانی بشود پرداخت غیر لمسی دارید و پرداخت های EMV پلاستیکی منسوخ میشود. به عوامل زیر توجه کنید:

- **نوار مغناطیسی بر روی نوار مغناطیسی وضعیت موجود را در تقلب حفظ میکند**

حتی بعد از تغییر قانون اگر هیچ کدام از صادرکننده یا فروشگاه(پذیرنده) پشتبانی EMV نداشته باشند ( ازنوع چیپ یا غیر لمسی) میزان امنیت برای تقلب تغییری نمیکند. در این حالت اگر فروشگاه(پذیرنده) همه اطلاعات لازم را از دارنده کارت بگیرد و همه قوانین را پیروی کند موسسه مالی متحمل مسئولیت تقلب خواهد بود. بنابراین اگر همه با هم انجام ندهند ( از کوچکترین صادرکننده گرفته تا فروشگاه(پذیرنده) ها به EMV ارتقا دهند) امنیت در همان سطح پایین می ماند. فروشگاه(پذیرنده) های کوچک با پرداخت های عمدتا شخصی به ندرت مورد تقلب قرار میگرند که بخواهیم 250 تا 600 دلار صرف ارتقا آنها بکنیم.

- **فروشگاه(پذیرنده) ها تمایلی ندارند که سریعا هزینه ارتقا ترمینال ها را بپردازند**

شرکت دیپات و تارگت برای جلوگیری از نفوذ داده ترمینال های فقط نوار معناطیسی را به چیپ های EMV و غیر لمسی ارتقا دادند. به علاوه لیست قسمت 250 تا 600 دلار که برای ترمینال های غیر لمسی و چیپ EMV ذکر شد شامل هزینه ارتقا شبکه نمیباشد. فارستر تخمین میزند که 11 تا 13 میلیون از پایانه های POS در آمریکا وجود دارد که EMV تنها 10 درصد نفوذ داشته است. بنابراین مبلغ

هنگفت 3 بیلیون USD برای ارتقا ترمینال ها بسیار بالاست. از این رو American express از فروشگاه(پذیرنده) های کوچک با 100 دلار حمایت میکند تا ترمینال های خود را ارتقا دهند

## کیف پول الکترونیک و پرداخت های موبایل با EMV پلاستیکی تصادم دارند

به خاطر مسائلی که در بالا توضیح داده شده فارستر انتظار ندارد که نه chip and pin EMV و نه EMV غیر لمسی پلاستیکی و نه chip and signature به راحتی مورد پذیرش گشترده در آمریکا واقع شوند . در ازای آن فارستر انتظار دارد که EMV غیرلمسی پلاستیکی و پرداخت موبایلی غیر لمسی ( یک کارت مجازی بر روی المان امن NFC ) و کیف های پول الکترونیک ( اپل پی و کیف پول گوگل) به شدت در رقابت با EMV پلاستیکی chip and signature و EMV plastic chip and PIN در بازار پرداخت آمریکا هستند. دلایل آن به شرح زیر است:

- **نفوذ گوشی های هوشمند در امریکا بسیار بالاست**

نزذیک به 72 درصد گوشی ها هوشمند هستند. که این بازار بزرگی است و فرصت ارتقا امنیتی خوبی برای تمام بازیگران زنجیره پرداخت تا به EMV پلاستیکی حرکت کنند. اتخاذ NFC در گوشی های هوشمند به سرعت با گوشی های اپل آیفن 6 و گلکسی اس 5 و دیگر گوشی های مشهور در حال گسترش است

- **هزینه شخصی سازی کارت های بر اساس گوشی از پلاستیکی ها کمتر است**

فارستر انتظار دارد که یکی از کارت های شرکت های visa mastercard American express بر روی یک المان امن در محیط قابل اعتماد از گوشی موبایل قرار گیرد. در این سناریو مشتری میتواند از چیپ NFC تعبیه شده بر روی کارت برای پرداخت غیر لمسی استفاده کند. و این هزینه صادرکننده ها را برای شخصی سازی (ساخت و برجسته کردن)و فرستادن کارت ها به دارنده کارت ها کاهش میدهد.

- **امنیت بالای گوشی های هوشمند و احراز هویت آنها امنیت پرداخت را بالا میبرد**

یکی از کاستی های سیستم های کارت پلاستیکی این است که احراز هویت دارنده کارت در بدون حضور کارت و با حضور کارت بسیار ضعیف است ( رمز 4 تا 8 رقمی هم برای به خاطر سپاری ساده است و هم برای استراق سمع) و پایانه های پرداخت میتوانند در خواست در نظر نگرفتن آنرا بدهند. گوشی ها حس گر خواندن اثر انگشت دوربین و میکروفون برای پارامتر های بیومتریک برای هم با حضور کارت و هم بدون حضور کارت دارند. بعلاوه GPS میتواند محدوده جغرافیای برای دارنده کارت ها در زمان پرداخت ایجاد کنند.

- **مدیریت تقلب در تراکنش های موبایلی قابل اعتماد تر و دقیق تر است**

پرداخت های بر اساس موبایل اطلاعات بیشتری همچون آی پی، آدری، مکان، داده های سنسور تولید میکنند و مدیریت تقلب میتواند از این داده ها استفاده کرده تا تصمیمات آنی بهتری برای استفاده از کارت پرداخت بگیرد. گوشی های میتوانند برنامه هایی چون پی پل را اجرا

کنند که توانایی مدیریت تقلب EFM را از تامین کنندگانی چون ACI و FICOو SAS افزایش میدهند تا مدیریت پرداخت بدون حضور کارت بدون اصطکاک انجام بشود.که از کلید های اساسی بخش EFM میباشد.

- **اکوسیستم بزرگ کیف پول الکترونیک و EMV غیر لمسی، استفاده از پایانه های غیر لمسی را اجباری میکند.**

اتخاذ اپل پی ، کیف گوگل، MCX ، CurrentC و کیف پول الکترونیک پی پل با اینکه با هم رقیب هستند فروشگاه(پذیرنده) ها را مجبور میکنند تا پایانه های POS کنونی را ارتقا دهند تا هم غیر لمسی ها و هم نوار های مغناطیسی و هم چیپ پشتیبانی بشود. وقتی پایانه های POS از کارت های غیر لمسی و NFC بر روی دستگاه های موبایل پشتیبانی کنند فارستر پیش بینی میکند که بسیاری از مشتریان آمریکایی از نوار های مغناطیسی به پرداخت های غیر لمسی کوچ میکنند

در پرداخت های موبایلی توکن کردن بسیار ساده و آماده است. ذخیره شدن شماره حساب مهترین مسئله در بسیاری از رخنه های اطلاعاتی مثل مورد سونی و شرکت Mandarin Oriental است. در حالیکه Current C ، پرداخت اپل ، کیف الکترونیکی گوگل اطلاعات را به صورت توکن شده در اینترنت منتقل میکنند در مورد EMV این مورد تازه در حال ظهور است. و با این سیستم ها فروشگاه(پذیرنده) هم نیازی به ذخیره شماره کارت ندارد و صرفه جویی در هزینه برای PCI-DSS داشته باشد. ولی متخصصان امنیت و ریسک باید توجه داشته باشند که فروشگاه(پذیرنده) میتواند اطلاعات PII مشتری را ذخیره کرده و توکن را به آن بچسباند و اطلاعات حساس مشتری را در اختیار داشته باشد.

*توصیه ها*

## از همه بازیگران زنجیره پرداخت بخواهید که توکن کردن را انجام بدهند

فارستر پیش بینی میکند که در سال 2015 در آمریکا، موبایل و EMV پلاستیکی غیر لمسی تراکنش بیشتری را به نسبت حجم تراکنش EMV Chip & pin و EMV chip & signature داشته باشند.S& R باید شتاب بیشتری را برای پرداخت غیر لمسی بدهد تا داده های مشتری بهتر حفظ بشوند و از رخنه انبوه جلوگیری شود.

- **فواید امنیتی و ریسکی برای فروشگاه ها(پذیرنده ها)، خرید ترمینال هایی با پشتبانی همزمان نوار مغناطیسی +غیر لمسی + چیپ را هموار میکند**

هزینه 250 تا 600 دلار برای هر ترمینال بسیار آزار دهنده است ولی اگر قانون ضد کلاهبرداری را به صادرکنندگانی که که در پذیرش EMV تاخیر دارند، تحمیل کنیم ، نتایج خوب امنیتی برای آنها در کنترل رخنه اطلاعاتی دارد.

- **فواید امنیتی و ریسکی برای صادرکنندگان، کارت های چیپ+ غیر لمسی را به اجبار وارد کنید اگر قبلا در گسترش ان تلاشی نکرده اید.**

اگر پایانه پذیرنده قبلا از EMV چیپ و یا غیر لمسی پشتیبانی میکند از اینکه هزینه تقلب را متحمل شوید جلوگیری میکند بعلاوه اگر میخواهید از دیگر پارامتر های تراکنش مانند مکان تراکنش هم بهره ببرید بهتر است از EMV استفاده کنید

- **فواید امنیتی و ریسکی برای همه ، تقاضای توکن کردن را داشته باشید**

در محیط نا امن کنونی ذخیره کردن شماره کارت به صورت رمز و یا غیر رمز شده غیر مسئولانه است . تنها با processor ها و پذیرندگانی کار کنید که پشتیبانی از توکن را برای جلوگیری از رخنه بی درنگ انجام بدهند.

## شیوه بررسی در این مقاله

Forcase view اتحادیه ای است که سالانه به بیش از 40 پیش بینی در آمریکای شمالی، اروپا، آسیا و آمریکای لاتین دسترسی دارد. پیش بینی یک روش منحصر به فرد دارد. یک بالانسی بین خواسته مشتر ی و داده هایی که دارد انجام میدهد و بررسی دقیقی از هر بازار ارائه میدهد. Forcase view فارستر بررسی و نگاه موثقی به تکنولوژی موبایل و آنلاین و مشابه آن دارد. و یک چارچوبی از جلوبرندگان و مهارکنندگان بازار ارائه میکند و به مشتریان کمک میکند اولویت سرمایه گذاری درست را اتخاذ کنند.و از مدل هایش داده های دقیق و پارامتر های بازار را که حاصل 5 سال کار تجارت الکترونیک ، کار با مشتریان ، سرویس های مالی ، موبایل ، آنلاین و بازار تعاملی است، در اختیار میگذارد. به عنوان بخشی از مدل پیش بینی فارستر بر اساس منابع گوناگون مستندات مالی عمومی ، مصاحبه ها و تخمین سالیانه و جامعی از اندازه بازار می زند.

همه پیش بینی های آن توسط تیمی اختصاصی که مدل ها را میسازند و تحقیقات فشرده فنی انجام میدهند و با هم به اجماع رسمی میرسند. افراد تحلیل گر فارستر که تجربه کاری در زمینه سرمایه گذاری بانکی، مشاوره مدیریتی و تحقیقات بازار دارند که کمک شایانی در پیش بینی های آنها میکند.

## کلمات اصلی و ترجمه

**فروشگاه(پذیرنده)- merchant**

**رخنه اطلاعاتی – breach**

**دارنده کارت – card holder**

**صادر کننده – issuer**

**پذیرنده – acquire**

**بدون حضور کارت – CNP**

**با حضور کارت – CP**

**قانون تغییر مسئولیت – liability shift**

**توضیح این قانون در ذیل آمده است:**

Some U.S. payment networks are implementing EMV fraud "liability shifts" effective October 2015. fast approaching, many card issuers, merchants, acquirers and processors With these liability shifts implementing EMV chip technology are asking, "Who is liable for what, and when, under these fraud 'liability shifts?' "The EMV Migration Forum is providing this information collected from certain payment networks to help payment industry participants better understand the corresponding network's .policies