CNP WHITE PAPER

FROM UNIVERSAL IDENTIFIER TO FRAUD BUSTER

Why Email Risk Assessment Has Become Indispensable to Your Business

CNPCardNotPresent.com®
THE INDEPENDENT SOURCE FOR ORIGINAL CNP NEWS

emailage™
GLOBAL FRAUD PREVENTION

FROM UNIVERSAL IDENTIFIER TO FRAUD BUSTER

Why Email Risk Assessment Has Become Indispensable to Your Business

"If you have the ability as a company to actually see the history and behavior behind an email address, that is one hell of a fraud indicator."

–Brett "Gollumfun" Johnson

Why does a former hacker and card-not-present fraud pioneer think email risk assessment could be the most important weapon in a business's antifraud arsenal? Because, it's the one identifying piece of information that accompanies every e-commerce transaction. And, because fraudsters prize efficiency just as any organization does.

As much as any single person can be held responsible for the proliferation of card-not-present fraud and the development of many of its most pernicious techniques, Brett Johnson is that individual. Under the screen name "Gollumfun," he and several other notorious cybercriminals established Shadow Crew, the very first online forum where hackers and fraudsters gathered to buy and sell stolen information and to trade tips, strategies and ever-evolving ways to monetize that information. When you hear the term "Dark Web," Shadow Crew is where it all began.

Johnson has traveled a winding road from celebrity hacker/fraudster to U.S. Most Wanted criminal to federal prisoner to ex-convict and reformed thief. Currently, he makes his living advising legitimate businesses how to protect themselves from people exactly like himself. He was a fraud innovator and spends lots of time in his old online hangouts keeping informed about how his former business has evolved. And, at this dangerous moment in time, Johnson is convinced that having a process in place to evaluate the risk of an email address associated with an online transaction or account is the most important thing a business can do to protect itself.

The Email Address as a 'Global Digital Passport'

Originally, businesses began collecting email addresses from customers or applicants to establish an open and direct channel of communication—a customer service play. Customers saw the utility and became comfortable supplying their email in all their online interactions. Companies quickly saw its value as an identifier.

From a digital perspective, two characteristics make it the best form of identification. It's ubiquitous: There are 2.7 billion active email users around the world (the next closest trackable account would be Facebook at 1.6 billion, which requires a valid email address to create an account). And, it's persistent: 91 percent of active email users have had the same address for at least three years and 51 percent have retained the same active email address for at least 10 years.[1]

FROM UNIVERSAL IDENTIFIER TO FRAUD BUSTER

Why Email Risk Assessment Has Become Indispensable to Your Business

According to Amador Testa, chief product officer for email intelligence provider Emailage, there is no single piece of data that can tell you as much about an online user as an email address.

"We truly see the email address as a person's global digital passport," Testa says. "Email works everywhere and everyone is on the same standard—a handle, an 'at' and a domain—regardless of where a person is in the world."

Creating a Fake 'Passport'

So, the utility of email for both online merchants and their customers became well established and email emerged as the one piece of information every transaction required. But, as the potential of e-commerce as a tool for fraud became apparent to the criminal element, another characteristic of email enabled thieves to accommodate that requirement: It is not hard to set up an email account. If every online transaction and every online account only needed a valid email address as identification, fraudsters would simply do what they have been doing in the physical world forever: create a fake ID.

From the first instance of card-not-present fraud to the current day, according to Johnson, the process for criminals monetizing stolen information online nearly always begins the same way: receive the stolen information and then create an email address.

"A fraudster's goal is to get the fraud score of a transaction a low as possible whenever they can," he explains. "To do that, he will buy a card and then generate an email with the name on the card 'at' some domain."

Johnson says he has aged email addresses in the past and others are probably doing that now, but most criminals want the name in the email address somehow associated with the name on the card. Fraudsters are keenly aware that generic handles raise more flags in a merchant's fraud screening than if the handle contains the same name as the payment instrument.

"Serious criminals research security companies," he warns. "They will see how those providers operate and try to identify which companies are actually gauging email addresses. So they are beginning to age them. That's the way seasoned fraudsters tend to work."

The domain is another area fraudsters leverage in an attempt to throw antifraud systems off the trail, Johnson says. A free email account from a service like Gmail, Yahoo or Hotmail is fine for legitimate customers with a host of other characteristics (e.g., a shipping address that's the same as the billing address) to fall back on that won't raise fraud flags. A fraudster

will be doing other suspicious things. As a result he (or she) will try to lower the fraud score of a transaction in any way he can. But while fraudsters may constantly create new emails, it's exceedingly rare for legitimate customers to do that.

Expert fraudsters are using .edu addresses or they have bought business domains based on existing businesses. In both cases—an e-commerce purchase by a student or by a business—a discrepancy between the shipping and billing address will not raise as many flags.

As always, fraudsters adapt. But, no matter what techniques they use, they can't avoid creating an email address. As Johnson points out, "email crosses the entire spectrum of cybercrime." Having as much visibility as possible into the history of the email address associated with an e-commerce order, loan application or bank account is vital. In fact, in Johnson's informed opinion, it's as fundamental to a company's security posture "as having a firewall and a password manager."

But how does a company come by that visibility?

Email Risk Assessment as a Service

When was the last time you opened an account or bought something online without an email address? It's nearly impossible. The email address has evolved as the unique identifier—the digital passport—of every online user. Merchants have quickly realized its potential for validating shoppers during e-commerce transactions. For a long time, however, this potential was unrealized, according to Testa.

"Merchants were collecting the email, but doing very little with it, from a fraud prevention point of view," he explains. "They were building white lists and black lists. Have I seen that email associated with a fraud event? Have I seen that email associated with a good customer? But that was only for returning customers. If a merchant had a new customer, the email didn't have much value from a fraud prevention perspective."

Eventually, merchants began asking more—and better—questions about the email addresses associated with their online transactions. Is this email valid and active? How long has it been active? When was it created? Has it been associated with a fraud event at another company?

Unfortunately, many of those questions remained unanswered. Companies did not have visibility into when emails were created, only when they had seen them for the first time. Nor did they know about fraud events outside their own company.

FROM UNIVERSAL IDENTIFIER TO FRAUD BUSTER

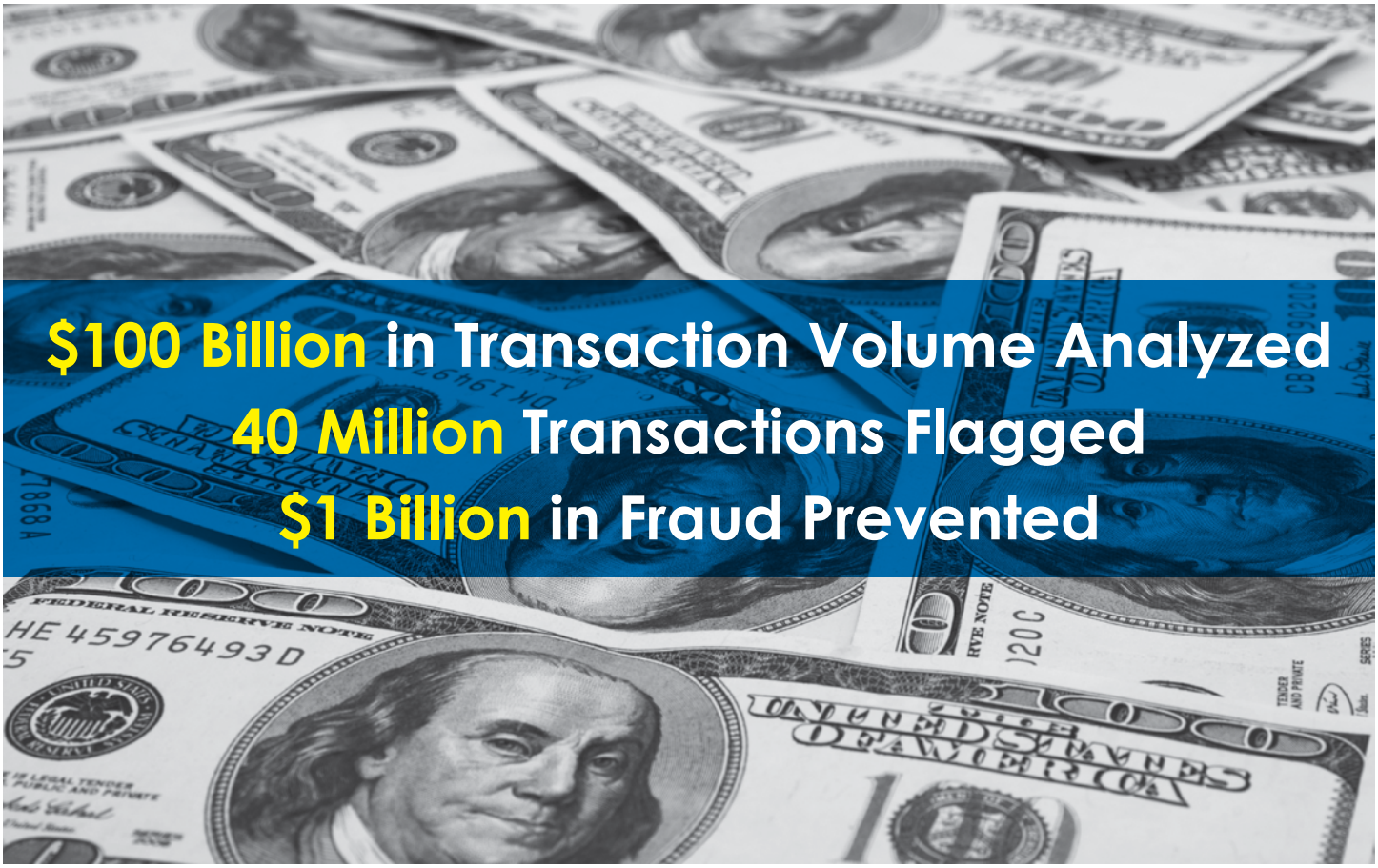
Why Email Risk Assessment Has Become Indispensable to Your Business

In the mid-2000s, Yahoo began sharing information on the validity and age of emails with merchants. But, while it was an incredibly welcome development, it only allowed businesses to investigate Yahoo emails and within a few years, Yahoo discontinued the service.

Enter Arizona-based Emailage.

Founded in 2012, Emailage was the first third-party service devoted strictly to amassing intelligence on email addresses. Through various partnerships, data sources and machine-learning technology, Emailage is able to build a historical profile associated with any email address and render a score predicting how trustworthy the user is.

What Emailage provides that companies cannot do for themselves, according to Testa, is scale and access to a network.



FROM UNIVERSAL IDENTIFIER TO FRAUD BUSTER

Why Email Risk Assessment Has Become Indispensable to Your Business

"Anyone can try to build intelligence on identity, on how long emails have been active, if they have been associated with Social activity or if they have been connected with fraud events," he says. "But, it is an intensely manual process for companies trying to do it themselves and they have limited visibility into some of the characteristics we track."

In addition to the age of an email address and the name of its owner, Emailage can tell what country it originated from, connect it with IP data, spot irregularities such as tumbling and more. Moreover, its algorithm can identify suspicious patterns due to the size of its network.

"There are plenty of companies out there assessing fraud risk... some are device driven, some are generic-data driven, some are based on machine learning. But we are able to tap all these technologies and connect those elements with email."

There's a flip side, too: the same process works with legitimate customers. When you can identify positive behaviors, you can approve those customers more quickly.

Among the more than 1,000 customers who rely on Emailage for email risk assessment are four of the six largest issuing banks in the U.S., five of the top 10 e-commerce retailers, three of the five biggest global airlines, the top three computer manufacturers and the top five P2P money transfer companies. Additionally, many more are part of the network through partnerships with the five largest antifraud platforms.

With visibility into the billions of transactions generated by companies using its service, every company connected to its network benefits from a holistic view of email risk. If an email is associated with a case of confirmed fraud at one of its customers, every customer is alerted. It is a powerful force multiplier.

"There are plenty of companies out there assessing fraud risk," Testa notes. "Some are device driven, some are generic-data driven, some are based on machine learning. But we are able to tap all these technologies and connect those elements with email."

FROM UNIVERSAL IDENTIFIER TO FRAUD BUSTER

Why Email Risk Assessment Has Become Indispensable to Your Business

Case Study: Abercrombie and Fitch

Introduction: Retail clothing brand Abercrombie and Fitch derived nearly one-third of its $1.04 billion in Q4 2016 revenue from the online channel. According to Senior Fraud Analyst Trent McGough, the company's main fraud concern centers around its e-gift card program. Since implementing Emailage, McGough says not only has A&F been able to prevent tens of thousands of dollars in e-gift card fraud per month, it has enabled the company to automatically approve thousands of orders per quarter that previously would have been held for manual review.

The problem: Several years ago, McGough and his team noticed a troubling increase in chargebacks associated with e-gift card purchases. They noticed some anomalies with the emails associated with e-gift card orders and began looking for ways to find out more information on those email addresses. At the time, Yahoo would share when its email accounts were created with merchants that asked for the information. A&F benefitted from that visibility, but only for Yahoo emails and only until Yahoo discontinued the service. McGough needed more information on the emails coming in on e-gift card orders.

The solution: McGough evaluated several providers and chose Emailage. Initially the retailer used the service on a per-click basis only for orders that had already been held for manual review. A&F's fraud team used Emailage to check the age of email accounts in those cases. Based on successes in that environment, McGough began testing in the fall of 2016 to evaluate expanding the service and adding it in a more automated way. Through testing, the company decided to use Emailage to automatically screen all orders flagged for manual review, all e-gift card orders and all orders in excess of $150.

The results: Testing revealed two effects.

1. Significantly more fraudulent activity, which previous controls would have approved, was caught
2. False positives involving legitimate customers were also reduced

In the first four months of 2017, McGough says Abercrombie and Fitch prevented nearly $150,000 of fraud that would have been approved under its old system. In addition, during the same time period, nearly 4,000 legitimate orders that would have been held for review were automatically approved with a low Emailage risk score.

Abercrombie & Fitch 2017 Fraud Data

	Fraudulent Orders Prevented	Manual Reviews Prevented
January	180	952
February	237	856
March	287	984
April	214	1,072

"We've seen a very compelling ROI from Emailage," McGough says. "We definitely expanded the program from where we started and we only did that because we found value in it. There have been a lot of times using the email address when I've been able to say they order looks strange, but then you figure out who it's registered to or that their information matches the name. Other times you find out an email was created two days ago. If the order already looked a little suspicious, it's very easy to reject the order using that. I've found email risk assessment is a good indicator of both positive and negative behaviors."

Conclusion

The email address has become the most important identifier attached to online activity. It's pervasive, a part of just about every login, transaction or account created or performed in the digital arena. And, while fraudsters try to adapt, there is no way around the fact that, to cash out, they must steal or create an email address.

As former fraudster Johnson notes, "Every single thing about the legitimacy of a transaction depends on the history and activity of an email address. And, the best way for fraudsters to work is to make an email account on demand. Right now, it's extremely vital for companies screening for fraud to have a system in place to evaluate email addresses as a risk factor."

FROM UNIVERSAL IDENTIFIER TO FRAUD BUSTER

Why Email Risk Assessment Has Become Indispensable to Your Business

About Emailage

As the global hub of email intelligence, the Emailage team has a singular goal: uniting companies in the fight against fraud. We harness the power of the email address to help our customers balance effective fraud detection with great customer experience. Companies across the globe use our predictive scoring on transactions of all types. Our network's constant growth enables 90% of fraud detected to be driven by attributes coming from our proprietary algorithms. Before Emailage was founded in 2012, companies relied on their own siloed technologies and databases to incorporate email in their fraud tools. This consisted mostly of manual processes, one-to-one comparisons and maintenance of internal blacklists. Emailage has changed the entire fraud landscape by breaking these silos with unparalleled global coverage and a commitment to unite companies in the fight against fraud.

About CardNotPresent.com

CardNotPresent.com, part of the RELX Group, is an independent voice generating original news, information, education and inspiration for and about the companies and people operating in the card-not-present space—one of the only sources of content focused solely on this growing segment of the payments industry. Our only product is information. Our only goal is to provide it in an unbiased manner to our subscribers. The company's media platforms include the CardNotPresent.com portal, the hub for news, information and analysis about the payments issues that most affect merchants operating in the space; the CNP Report, an e-newsletter delivering that focused information directly to your email inbox twice a week with no extraneous clutter; the CNP Expo, an annual gathering of the leading companies in the space from the smallest e-commerce Websites and technology providers to global retailers and payment processors; and the CNP Awards, an annual event honoring the products and solutions CNP merchants rely on most to increase sales. For more information, visit www.CardNotPresent.com.

This document was produced *as a joint effort* between CardNotpresent.com and Emailage.

FOOTNOTES

1. DMA Insight: Consumer email tracking study, 2015
https://dma.org.uk/uploads/56543b6e6d645-email-tracking-report-2015_56543b6e6d5b5.pdf