Synthetic Identity Fraud: A Look Behind the Mask

When credit and debit card issuers in the United States began rolling out Europay, Mastercard and Visa (EMV) chip cards, card counterfeiters saw the handwriting on the wall. EMV would ultimately crimp their ability to use counterfeit cards at the point of sale, so they migrated to other forms of fraud, such as card-not-present transactions in online channels.

Many others became more creative. They have turned to creating phony identities pieced together with information from several real and fictitious sources. The crooks often concoct batches of non-existent "synthetic identities" by combining stolen or made-up Social Security numbers (SSNs) with an assortment of addresses, names, phone numbers, and dates of birth. Perpetrators can then use the synthetic identities to apply for credit, make major purchases, or take other actions that help give each identity a financial history.

With the proliferation of digital commerce, synthetic identity fraud has steadily grown to become one of the predominant tactics of fraudsters — especially in "faceless" channels. Synthetic identity credit card losses are notoriously difficult to track, but in 2018 Aite Group estimated U.S. losses will soar from $580 million in 2015 to $1.25 billion in 2020.

Julie Conroy, research director for Aite Group's Retail Banking practice, calls synthetic identity fraud "the new elephant in the room — a problem that is rising to epic proportions but that many have yet to acknowledge."

In addition to EMV chip cards gaining traction in the U.S. Aite Group named three other factors driving the growth of synthetic identity fraud: rampant data breaches, randomized SSNs, and looser credit standards. Another major catalyst to this crime is the increased abuse of authorized user privileges on credit card accounts. Let's explore this further.

Authorized User Abuse: A Major Synthetic Identity Fraud Catalyst

Issuers of credit cards have long allowed primary account owners to add other people to their accounts. Ordinarily, authorized users are real people with legitimate needs for a credit card. Most are family members, and that's one reason why financial institutions don't discourage credit card account owners from adding authorized users. The practice enables a spouse or a child to establish credit or overcome a bad credit history by tapping into the primary account owner's credit history.

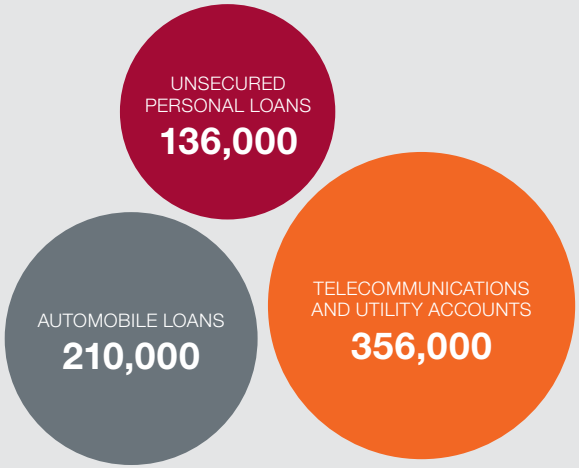
Authorized user accounts are very profitable for card issuers, but criminals are now exploiting how easy it is to get authorized user status. Read on to learn how criminals create synthetic identities, capitalize on the primary account holder's good credit history, and ring up huge losses for issuers.

Synthetic Identities Don't Stop with Credit Cards.

The credit card industry is definitely the fraudster's favorite target. Internal studies of top card issuers revealed that within just a year's time, 1 million accounts were identified as potentially synthetic.

However, Equifax data shows that synthetic identity fraud extends far beyond credit cards. Here's a snapshot of what we're seeing in other areas:

Accounts flagged over 12 months as potentially synthetic:



Observed behaviors of fraudsters using synthetic identities

- Often move from auto loans to other non-card loans
- Little SSN verification evidence
- Hyper-monitoring of credit
- No proof-of-life evidence
- Shared SSNs

STEVE GREEN

Granted authorized
user privileges

MOLLY EMERSON
"Helen Day"

The Birth of a Fraud Ring

Steve Green* is a consumer who has tradelines in Equifax data files. In 2017, he was in good standing with a high credit score and positive credit histories on six accounts.

But Equifax detected a darker side to Steve that wasn't evident from his credit score or payment history. His good credit was being used to father a fraud ring.

What follows are the three key steps that fraudsters take — with help from enablers like Steve Green — to create and exploit synthetic identities: Fabrication, Legitimization, and Action.

FABRICATION: How synthetic identities are created.

A fraudster, Molly Emerson*, creates new identities. First, she makes up an SSN or steals one from a deceased person, a child, or a data breach victim whose stolen credentials have been sold on the black market.

Next, she fabricates a name — for example, "Helen Day" — and a date of birth to be used with that SSN. She adds a mailing address, and perhaps provides an email account or an untraceable phone number.

Then, Molly applies for a low-limit credit account using her new fake identity, "Helen Day." The bank or retailer submits an inquiry to a credit reporting agency about Helen Day's credit history. The application will probably be denied because a profile matching Helen does not exist. Even so, as required by the Fair Credit Reporting Act, the credit inquiry generates a credit profile of Helen Day in reporting agencies' databases — and that's a win for Molly.

*Names in this document are fictitious and do not represent real people.

1

A fraudster, “Molly Emerson,” steals an SSN.

2

Molly creates a synthetic identity, “Helen Day”

NAME & DOB
Helen Day
03/24/1976

ADDRESS
123 Main Street
City, FL 30034

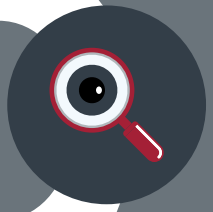
STOLEN SSN
123-456-7890

3

APPLICATION

“Helen Day” applies for a credit card.

4



Bank sends inquiry to reporting agency.

5

Credit reporting agency adds a profile for “Helen Day”

HELEN DAY
123-456-7890

HELEN DAY

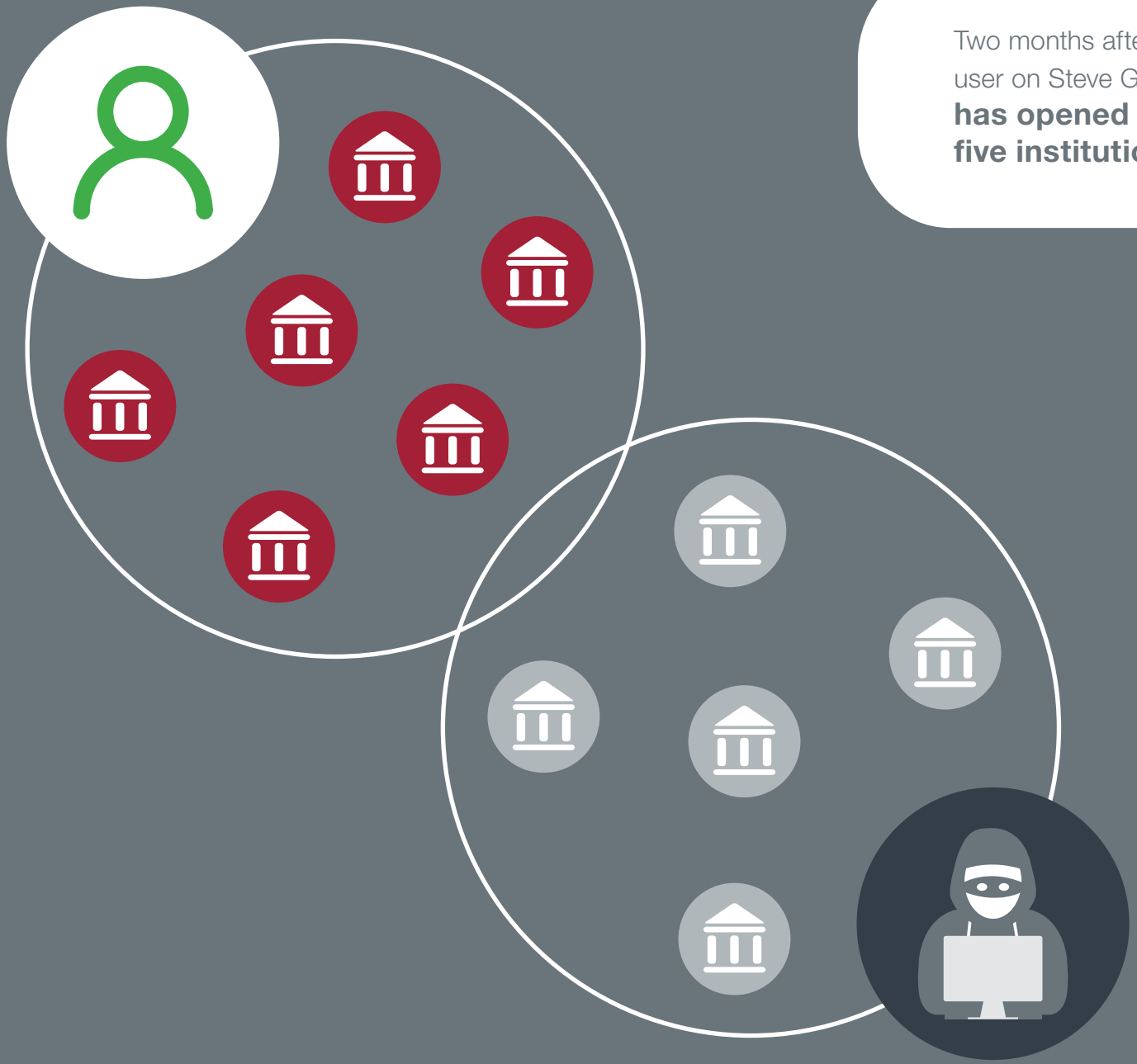
LEGITIMIZATION: How fake identities gain the appearance of real people.

To gain real traction on the fake identity, Molly pays a primary card owner, such as Steve Green, to add Helen Day as an authorized user to his account for a defined period.

Molly has agreed will she will not incur charges on Steve's account. Steve continues making timely payments for any charges he made on this account. So, each month, Steve's card issuer relays positive account information about Steve Green — and Helen Day — to credit reporting agencies.

In essence, the scheme enables the synthetic identity, Helen Day, to inherit the benefits of Steve Green's good credit profile. Molly then attempts to gain lines of credit with Helen Day's newly established positive credit history.

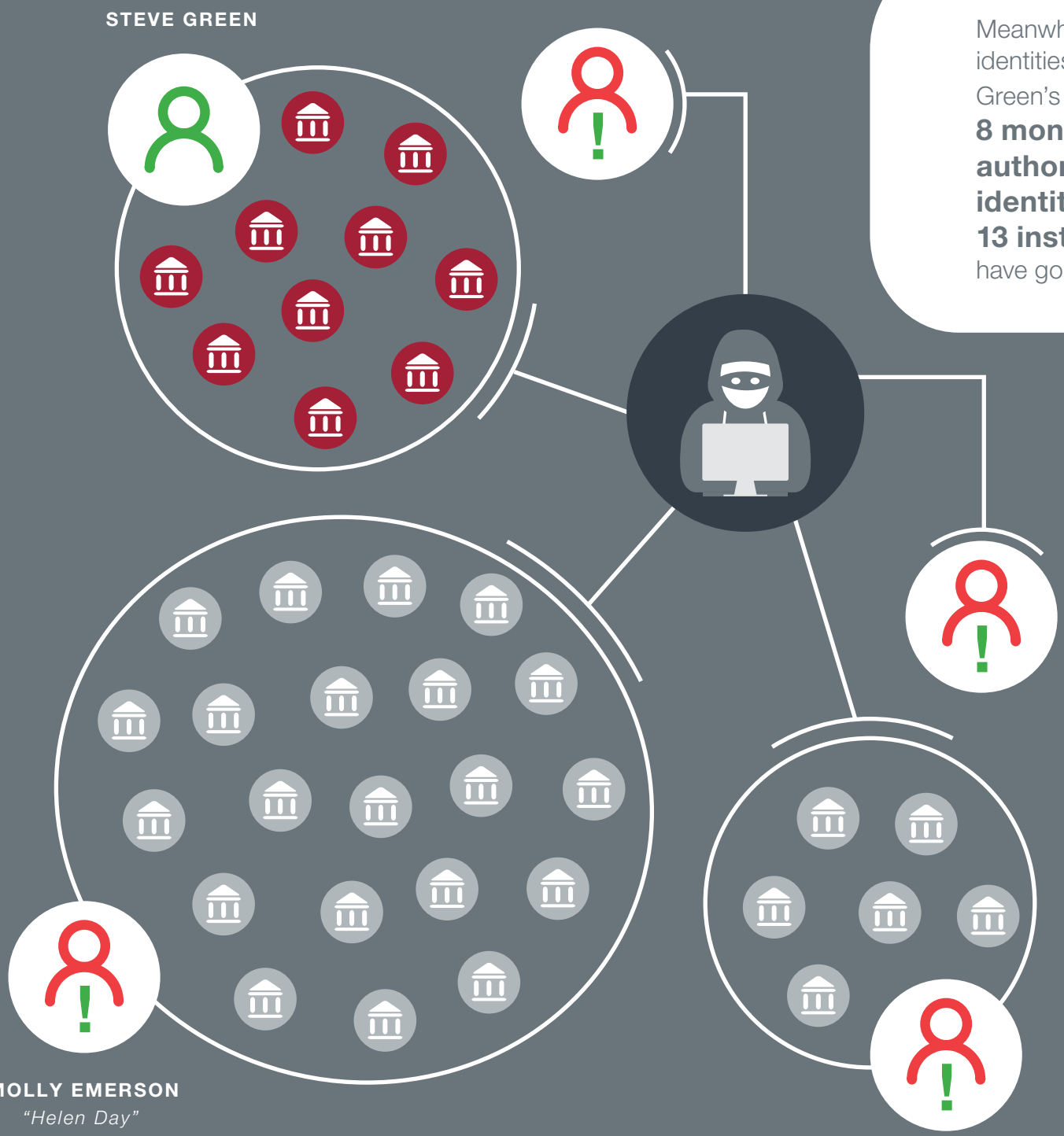
STEVE GREEN



Two months after becoming an authorized user on Steve Green's account, **"Helen Day" has opened five accounts at five institutions.**

MOLLY EMERSON

"Helen Day"



Meanwhile, Molly is creating other synthetic identities, some of which she adds to Steve Green's account as authorized users. **After 8 months, Steve's account has four authorized users that are synthetic identities, opening 28 accounts at 13 institutions.** None of the accounts have gone delinquent yet.

Authorized user abuse is just one avenue fraudsters use to nurture their fake identities. Many will sign their synthetic identities up for utilities, TV services, furniture rentals, secured credit cards, or pre-paid phone accounts. These are all products typically marketed to consumers who are new to credit.

Gradually, the fraudsters increase the credit limits on already-opened accounts and move up to larger account requests. They use the synthetic identities to apply not only for more credit cards, but also for auto loans, installment loans, and even mortgages. A synthetic identity's newly opened accounts may go many months before a fraudster taps into available funds because other accounts are still being opened under the same identity.

ACTION: The fake identities "bust out" and bilk lenders.

Over a period of 22 months, Molly has patiently nurtured "Helen Day" and other synthetic identities into people who, she hopes, will look real to lenders and credit reporting agencies.

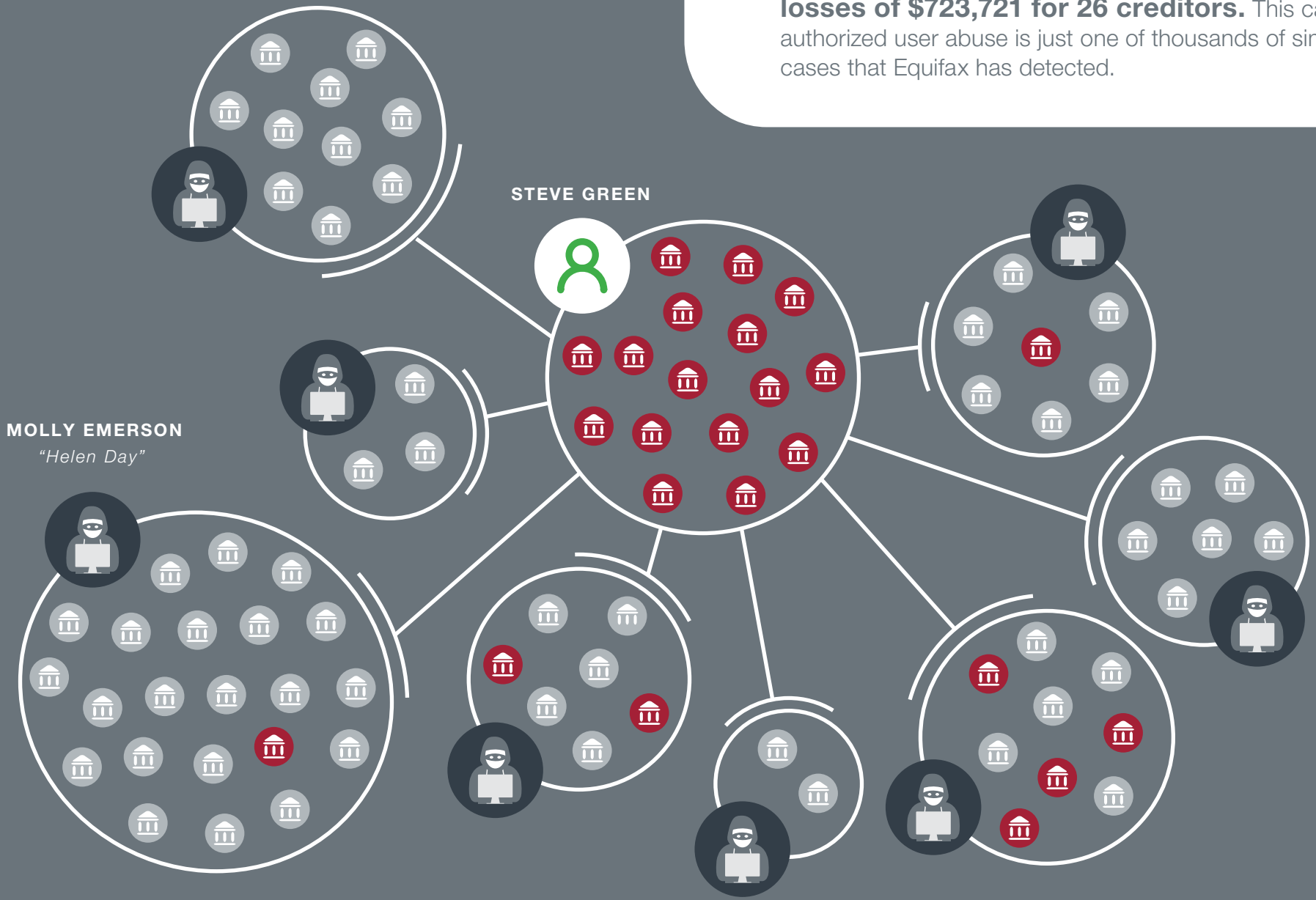
Helen Day and Molly's other synthetic identities have now graduated from being Steve Green's authorized users. Their falsified identities have become legitimized — so Molly monetizes them with a "bust out." Molly's phony identities charge the maximum on all accounts with no intention of making payments. When the bust out occurs — typically about five months after becoming an authorized user, but often much longer — creditors are generally left with significant losses and no responsible party to chase in their collection and recovery processes.

The Achilles Heel of Synthetic Identities

In the credit world, the characteristics identifying real people don't suddenly appear in the public domain a few months before they start applying for credit. Real people leave digital and documentary evidence of their existence throughout their lives. They register vehicles. They have relatives. They have employment histories. They have current and previous addresses. They have court appearances. They pay for utilities and cell phones. They may have student loans or secured credit cards. They have email addresses and social media accounts.

When few of these identifiers seem to exist, that could be a red flag for synthetic identity fraud.

Almost two years after Steve Green began collaborating with fraudsters, one of his credit card accounts has become a launching pad for synthetic identity fraud. Steve's account helped legitimize **eight synthetic identities who opened 66 fraudulent accounts that generated losses of $723,721 for 26 creditors.** This case of authorized user abuse is just one of thousands of similar cases that Equifax has detected.



Fighting Synthetic Identity Fraud

The conventional fail-safes for detecting fraudulent accounts are rarely effective with synthetic identity fraud.

Real people won't see activity on synthetic identity accounts created with their SSNs because there are no matching names and addresses. Therefore, they won't raise any red flags. If a bank's security department calls with questions about suspicious activity, the fraudster will simply say the transactions are legitimate.

As demonstrated in the previous sidebar titled Synthetic Identities Don't Stop with Credit Cards, many categories of lenders are vulnerable to synthetic identity fraud. How can financial institutions and other lenders affordably mitigate the risks of synthetic identity fraud without encumbering legitimate customers with unnecessary checks and manual reviews?

In 2017, the U.S Government Accountability Office convened a panel of 14 experts to advance the national dialog on synthetic identity fraud. Panelists agreed that credit reporting agencies and data brokers are positioned to have the best information for detecting synthetic identity fraud suspects because they collect massive amounts of information from financial institutions. Their data can often signal the creation of a synthetic identity or other SSN-related fraud at account opening — before any damage is done.

Credit reporting agencies and data aggregators offer robust, reliable countermeasures for detecting synthetic identity fraud. Integrated solutions, delivered in batch processing or real-time mode, can combine verification, authentication and fraud detection technologies. Predictive tools, such as fraud scores, can be tailored specifically to an organization's business needs.

There are three different approaches solution vendors can use to address synthetic identity fraud:

1. **Authorized User Velocity.** Identifies suspicious primary account owners by monitoring how many authorized users become associated with a primary account owner over a short period.

2. **Identity Discrepancies.** Pinpoints mismatches between certain identity elements that can be a tip-off to fraud.

3. **Identity Confirmation and Behavior Analytics.** Uses a variety of data sources, both public and proprietary, to analyze behavior patterns and confirm identities.

Each approach is effective, but a combined approach performs best. For best results, your organization can combine services from these external resources with your team's internal anti-fraud processes.

Four Keys to Fighting Back

1

For countermeasures appropriate to your organization, supplement your internal anti-fraud tools with the multi-dimensional data resources of credit reporting agencies and data aggregators specializing in fraud. Their information will uncover “proof of life” behavior characteristics of legitimate applicants. (See The Achilles Heel of Synthetic Identities.) Combining this with machine learning (in step 3) provides a more fortified defense.

2

Use fast, reliable identity verification techniques that check applications against multiple sets of public and proprietary data. For example:

- Is the applicant’s address real?
- Does the applicant have an employment record?
- Does the applicant have utility or telecom accounts?
- Does the applicant have identifiable family members?
- Has the applicant registered a vehicle?

3

Machine learning algorithms can help discover identity discrepancies and unique behavior patterns, such as authorized user abuse, that may transcend multiple accounts at multiple creditors. This can help increase detection rates while lowering false positives -- in essence, providing a better experience for the consumer.

4

Use data analytics to detect linkages and suspicious patterns indicative of phony or manipulated identities. One example: by comparing an SSN to a consumer’s PII, algorithms can determine how well a supplied SSN matches its identity. A positive SSN confirmation along with several negative alerts can signal the creation of a synthetic identity or other SSN-related fraud at account opening.

A Closer Look at Helen Day

Data analytics can reveal striking evidence of suspicious activity and fraud before and after a “bust out” occurs. For example, if we look at Helen Day’s behavior for 22 months leading up to a bust-out, we see that she checks her credit score more often than the average consumer — five times more per month. We also see a higher volume of credit inquiries over a short period of time. This is not common for legitimate borrowers.

Volume of Credit Checks and Credit Requests Over 22 Months

HELEN DAY

Credit Checks

Credit Requests

AVERAGE CONSUMER

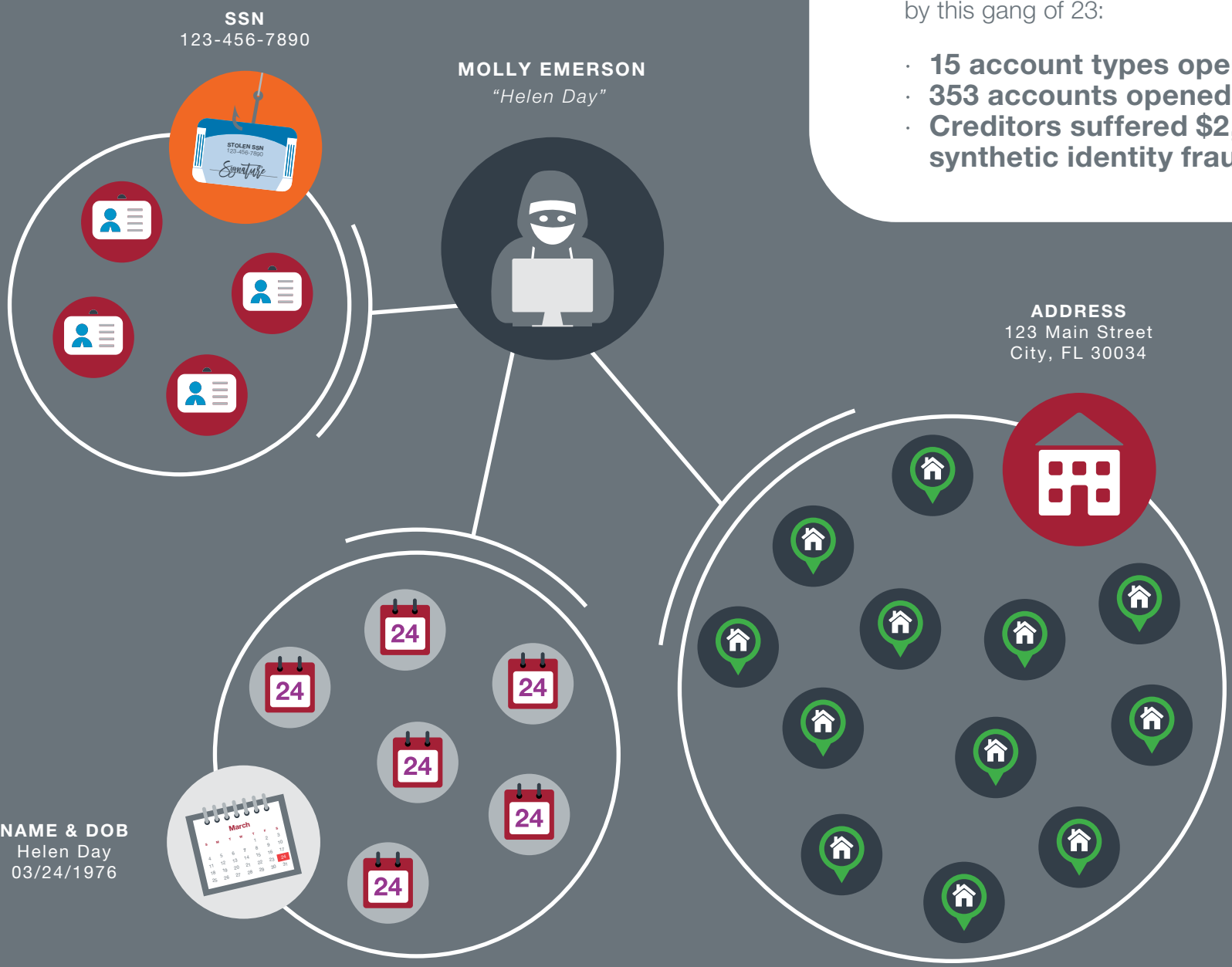
Credit Checks

Credit Requests

Fraudsters often use the same address on many established synthetic identities, but change addresses frequently. On average, “good” accounts change addresses only once every 70 months, while “bad” accounts change addresses every 10 months.

Collectively, **23 synthetic identities are sharing information used for identity verification.** Check out the mayhem caused by this gang of 23:

- **15 account types opened**
- **353 accounts opened**
- **Creditors suffered $2,582,432 in synthetic identity fraud losses**



How Equifax Can Help

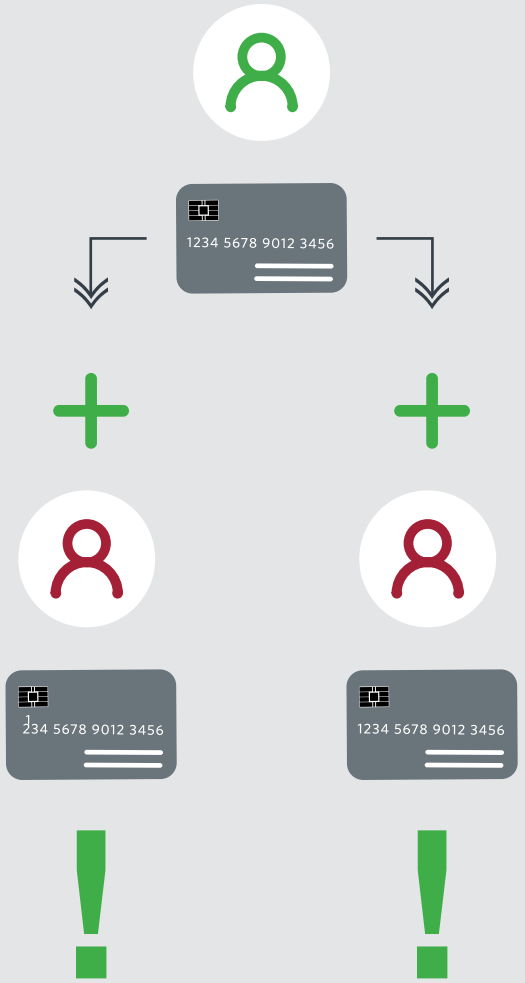
In 2018 Equifax launched an advanced approach for combatting synthetic identity fraud. FraudIQ® Synthetic ID Alerts use patent-pending machine-learning algorithms to detect synthetic identity behaviors and patterns at various entry points.

Delivered in batch or real-time, the alerts help determine if the identity presented is potentially synthetic, allowing you to:

- Leverage more actionable insights while maintaining low false positive rates
- Evaluate various patterns with advanced matching logic, such as authorized user/credit abuse, identity discrepancies, fraud/identity manipulations
- Analyze potential synthetic identity behaviors and patterns revealed by reliable, multi-dimensional data sources
- Better assess portfolio-specific risk, such as Credit Card, Automotive, Communications/Utilities, and Personal Loans

FraudIQ Synthetic ID Alerts can also be used as a screening tool with demand deposit accounts, which fraudsters often open as a foot-in-the-door to get other lines of credit.

To enhance the performance of FraudIQ Synthetic ID Alerts, Equifax can help you design a layered fraud defense to employ throughout an account's lifecycle — from marketing and account opening, through credit decisioning, account management, loss classification, and collections/recovery. For details, contact your Equifax representative or click here to request more information.



About Equifax

Equifax is a global data, analytics, and technology company. We believe knowledge drives progress. We blend unique data, analytics, and technology with a passion for serving customers globally, to create insights that power decisions to move people forward. Headquartered in Atlanta, Equifax operates or has investments in 24 countries in North America, Central and South America, Europe and the Asia Pacific region. It is a member of Standard & Poor's (S&P) 500® Index, and its common stock is traded on the New York Stock Exchange (NYSE) under the symbol EFX. Equifax employs approximately 11,000 employees worldwide.